EXHIBIT 7

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

ANIBAL RODRIGUEZ, SAL CATALDO, JULIAN SANTIAGO, and SUSAN LYNN HARVEY, individually and on behalf of all other similarly situated, Plaintiffs, v. GOOGLE LLC, Defendant.	No. 3:20-cv-04688-RS

REBUTTAL EXPERT REPORT OF JOHN R. BLACK, PH.D.

May 31, 2023

I. INTRODUCTION

A. Executive Summary

There is a fundamental disconnect between the technical expert report put forward by the Plaintiffs in this case and Google's technology as it is actually designed and used by Google. This disconnect underlies each of Mr. Jonathan Hochman's opinions in his March 22, 2023 expert report, and undermines them factually and methodologically.

I have reviewed the same evidence Mr. Hochman reviewed, the data Google produced in this case, the testimony of Google witnesses and Google internal documents, and conclude that Mr. Hochman fails to understand Google's technology, and that Google designed the at-issue technology at each step to protect user privacy and honor user privacy settings, including the supplemental Web & App Activity (sWAA) setting at the center of Plaintiffs' claims.

In particular, t Plaintiffs alleged that Google was supplementing marketing profiles with data collected by Google when users had turned sWAA off. I have not seen evidence of that. Even Mr. Hochman concedes that Google does not engage in ad personalization using sWAA-off data gathered from the at-issue products. He does opine that, as a semantic matter, the basic functioning of online advertising is a kind of "targeting" that would not be possible if Google honored users' sWAA settings. I explain in my report why this opinion is factually, technologically, and logically erroneous. In summary: the sWAA button is not described as an ad blocker, and does not function as one, but it does prevent Google from saving a user's app activity on third party mobile apps to their Google Account so that Google can use it in the future to better target that user with advertising.

Users, advertisers, and app developers are all informed of the various technological features at issue through Google's Privacy Policy, the terms of use for Firebase and Google's ads products, and through app developers' privacy policies. In my opinion, the technical process

described by Google in its WAA and sWAA setting descriptions is what Google does behind the scenes. I have not identified any technological disconnect between what Google represents on its WAA and sWAA web pages and what it does with user data received from the at-issue products: Google Analytics for Firebase, AdMob, and Ad Manager.

Further, it is my opinion, contrary to Mr. Hochman's, that Google goes above and beyond the necessary steps to honor user privacy settings, and takes affirmative, burdensome steps to mitigate joinability risk, or the risk that a bad actor could misuse Google's systems to "unmask" an individual. While no system is risk free, Google takes extraordinary steps to try to eliminate that possibility.

Finally, it is my opinion that Mr. Hochman fundamentally misunderstands the technology underlying how Google measures ad performance when he opines that Google monetizes sWAA-off data. While Google does measure ad performance for advertisers using basic ad record data, it does not monetize sWAA-off app activity data.

B. Qualifications

1. My name is Dr. John R. Black, Jr. I am an Associate Professor of Computer Science at the University of Colorado, Boulder. I received a B.S. in Mathematics and Computer Science from the California State University at Hayward (now "California State University, East Bay") in 1988. I received an M.S. in Computer Science in 1997, and a Ph.D. in Computer Science in 2000, both from the University of California at Davis ("UC Davis"). I have taught more than 60 classes in computer science, on subjects including data structures, algorithms, networking, operating systems, software engineering, security, cryptography, discrete mathematics, and quantum computing. I have authored or coauthored more than 20 publications,

primarily on issues relating to computer security. I have been involved with computers for over 35 years in both commercial and academic capacities.

2. My earliest interest was in networks and security. My first memories in this regard were around 1975 when a group of friends and I learned about the telephone network and its security. A few years later, personal computers became available and I spent most of my free time studying, programming, and modifying them. I worked extensively with various networking products throughout the 1980s, and developed an interest in cryptography soon thereafter. Although my undergraduate institution had no courses in cryptography or security in the 1980s, I decided to pursue self-study at the time, and opted to double major in Computer Science and Mathematics because cryptography is a blend of these two subject areas.

3. After earning my B.S. degree in 1988, I worked for six years at Ingres Corp as a software developer. My work primarily was directed at transaction logging, data type support, and security.

4. In 1995, I began my Ph.D. at UC Davis under cryptographer Phillip Rogaway. My area of focus was cryptography and security and my research involved encryption, authentication, hash functions, and network security. My Ph.D. thesis focused on authentication specifically, and portions of my thesis have been published as papers in top-level venues.

5. After graduation I took a position as an Assistant Professor at the University of Nevada at Reno. In the Fall of 2001, I taught the networking class there, which included coverage of Ethernet, interior gateway protocols, exterior gateway protocols, ARP, DHCP/BOOTP, IP, UDP, TCP, HTTP, SMTP and other protocols. In 2001, a graduate student and I looked at the security of ARP and invented a new protocol "AuthARP" to add security to the protocol.

6. In 2002, I moved to the University of Colorado at Boulder where I am currently employed. In the Fall of 2002, I co-designed and co-taught a new course called "Foundations of Computer and Network Security," which included descriptions of security issues around both wired and wireless security challenges, mostly for public-facing network services including the world-wide web. I have taught this class seven more times since then, including modern topics such as wireless networking, the Internet of Things, and so forth.

7. In my career at the University of Colorado, I have published several more papers in the area of cryptography and network security. I have taught more than 30 courses in network security and cryptography, and have graduated several PhD students in these areas. I have also served as a reviewer and referee for over 100 papers in the area of cryptography, including serving on more than 20 conference committees reviewing submissions to cryptography conferences. In 2009 I was the general chair of the CRYPTO conference.

8. I also worked as a consultant at times, often writing software on contract basis. Although most projects are covered by NDAs, many involved computer security and cryptography.

9. In 2011, I began technical consulting for a local company called Cardinal Peak, which focuses primarily on video encoding and delivery systems. My work for Cardinal Peak has largely been directed to video encoding, transcoding, compression, encryption, and DRM.2 For example, I designed the security system for the Pro1 smart thermostat, implemented the DRM for the Yonder Music App, worked on 802.1X code for smart dog collars, and helped design the cryptography used in Fitbit devices for wireless transfer of a Fitbit watch to a phone or laptop.

10. In 2016, I took a leave of absence from the University of Colorado to start a company called "SecureSet" in Denver, Colorado. The objective of SecureSet is to take reasonably proficient technical people and turn them into computer and network security specialists via five months of intensive training. SecureSet was sold to WeWork in 2019 and continues to offer computer security classes today.

11. A copy of my complete *curriculum vitae* is attached as Appendix A.

C. Assignment

12. I have been retained by Willkie Farr & Gallagher LLP ("Counsel") on behalf of Google, LLC ("Google" or "Defendant")[1] in connection with the matter of *Anibal Rodriguez, et al., v. Google, LLC*, pending in the United States District Court for the Northern District of California. I have been asked to review the expert report of Jonathan E. Hochman, who has submitted an expert report on behalf of Anibal Rodriguez, Sal Cataldo, Julian Santiago, and Susan Lynn Harvey ("Plaintiffs"), and provide my expert opinion as to Mr. Hochman's analysis of the technology and practices at issue in this litigation.[2]

D. Report Preparation

13. My billing rate for time spent on this matter is $625. My compensation is not contingent in any way on the nature of my opinions or the outcome of this litigation.

14. In forming my opinions, I have reviewed materials, data, and information provided to me by counsel or obtained from public sources. These materials include, among others, the Fourth Amended Complaint, Hochman Report, the documents Mr. Hochman cite in

[1] *Anibal Rodriguez, Sal Cataldo, Julian Santiago, and Susan Lynn Harvey, individually and on behalf of all other similarly situated, v. Google, LLC*, Fourth Amended Complaint, 3:20-cv-04688-RS, January 4, 2023 ("Complaint"), ¶ 2.

[2] *See* Expert Report of Jonathan E. Hochman, March 22, 2023 ("Hochman Report"). My decision not to respond to any one of Plaintiffs' expert's opinions in this report should not be construed as an endorsement of that opinion.

his report, documents the parties produced in the case, deposition testimony of various Google employees, deposition testimony of the named plaintiffs, and various data and publications from publicly available sources. The facts and data which I have relied on in forming my opinions are identified in this report, accompanying exhibits, and/or in Appendix B.

15. Certain factual bases from Mr Hochman's opinion are based on conversations he states he had with Mr. Lasinski, Plaintiffs' damages expert[3] Mr. Hochman did not disclose the substance of conversations in any of his report materials, so I cannot opine as to the accuracy or reliability of the information relayed in those conversations. I understand that Google's counsel requested notes or other documentation of these conversations from Plaintiffs' counsel but Plaintiffs' counsel refused to provide any, and instead, encouraged Google's counsel to discover their content through the expert deposition process. Consequently, I reserve the right to supplement this report and my opinions if, through deposition, Mr. Hochman reveals more information about these conversations.

16. I further reserve the right to adjust or supplement any opinions, as appropriate and permitted by the Court, should additional relevant documents or data become available.

II. BACKGROUND

A. Case Background

17. I have reviewed the operative complaint in this matter, and understand that Plaintiffs' have brought this action under the Comprehensive Computer Data Access and Fraud Act ("CDAFA") and under common law claims for Invasion of Privacy and Intrusion Upon Seclusion.[4] The complaint alleges that Google collected and saved data from users that had paused two specific settings: "Web & App Activity" ("WAA") and its sub-setting "supplemental

[3] *See, e.g.* Hochman Report, ¶ 33.
[4] Complaint, ¶ 226, pp. 69-75.

Web & App Activity" ("sWAA").[5] The complaint claims this collection was facilitated through Google Analytics for Firebase, a tool that app developers can install to gain analytics insights from Google about users' app interactions.[6] Finally, the complaint alleges that Google profits off this "WAA-off" and "sWAA-off" data through personalization, ad targeting, and analytics services.[7]

B. Key Technologies and Services

18. There are a number of technologies and services central to Plaintiffs' allegations. Below, I briefly define and describe those most vital to this opinion.

19. ***Firebase*** is a platform developed by Google for creating mobile and web applications. It provides tools and services to help app developers build, improve, and grow their apps easily.[8] Firebase offers its developer customers a range of services, including realtime databases, authentication services, cloud storage, hosting, and machine learning capabilities.[9] It helps developers simplify tasks that they may not have the overhead to handle in-house.

20. ***Google Analytics for Firebase* (*GA4F*)** is a free app measurement solution provided by Firebase. It provides app developers with insights on app usage and user engagement, which allows them to make informed decisions on their apps.[10] With GA4F, an app developer can measure various "events," or specific types of user app interactions. App developers can use these events to better understand user behavior and performance metrics.[11] It allows developers to understand how people use their apps, where they are encountering issues, and what actions they're

[5] Complaint, ¶ 1.
[6] Complaint, ¶¶ 1-4.
[7] Complaint, ¶¶ 137-140.
[8] "Firebase," Google, available at https://firebase.google.com.
[9] "Firebase Solutions," Google, available at https://firebase.google.com/solutions.
[10] "Google Analytics," Google, available at https://firebase.google.com/docs/analytics.
[11] "Google Analytics," Google, available at https://firebase.google.com/docs/analytics.

taking.

21. GA4F also offers its event measurement solutions through an integration with AdMob. ***AdMob*** is a mobile advertising platform by Google that helps place ads on developer's apps.[12] By integrating AdMob, a developer can create space and select the type of ads that will be displayed on the app.[13] AdMob then accesses Google's ad networks to bid on and display ads within those spaces. The integration between AdMob and GA4F allows app developers to measure various events related to users' interactions with the apps' ads. The integration additionally allows an app developer to view and analyze the user engagement data provided by Google Analytics for Firebase alongside the app monetization data provided by AdMob in a single unified platform. The purpose of this integration is to give developers a holistic view of their app's performance. It allows them to understand the relationship between user behavior and ad revenue, which can help them make more informed decisions about user experience and monetization strategies.

22. Both GA4F and AdMob rely on ***Software Development Kits***, **or** ***SDKs***. These are software tools and libraries that web and app developers use to create applications for specific platforms. An SDK functions as a bridge between applications and the platform they're built on. It contains libraries of code, documentation, and other resources. App developers can use these tools to simplify complex coding tasks and integrate specific features or capabilities, such as connection to a service like Google Analytics for Firebase. An app developer makes the decision to use an SDK. They may choose based on the app's requirements, desired functionalities, and the platforms they're developing for.

23. ***Firebase SDK*** is the SDK that app developers use to incorporate Firebase products,

[12] "What is AdMob," Google, available at https://admob.google.com/home/resources/what-is-admob/.
[13] "What is AdMob," Google, available at https://admob.google.com/home/resources/what-is-admob/.

including Google Analytics for Firebase, into their app.[14] ***Google Mobile Ads SDK*** is the SDK app developers use to access Google's various AdMob offerings.[15] Through Google Mobile Ads SDK, app developers can access certain features of GA4F, but to take advantage of the full integration between the two products, a developer would have to install both SDKs into their app.[16]

24. Separate from its developer-facing app analytics products, Google allows users to create ***Google Accounts*** as part of its user-facing products and services. Google provides users with Google Accounts to access many of Google's password-protected services, like Gmail, Google Drive, and Google Docs, and to download apps from the Google Play Store.[17] Users can also take advantage of using a single Google Account to link various Google services, such as through syncing Gmail with Google Calendar.[18] And, they can also "help[] you do more by personalizing your Google experience[.]"

25. A user signed into their Google Account can set personalization preferences through the Account's "Privacy & Personalization" settings. Here, they can manage "***Activity Controls***." Google explains that "[t]he data saved in your account helps gives you more personalized experiences across all Google services"and prompts users to "[c]hoose which settings will save data in your Google Account."

26. The ***Web & App Activity (WAA)*** control in Google Account is an optional setting that, when enabled, allows Google to save a user's searches and other activity on Google-owned

---

[14] "Add Firebase to your Apple project," Google, available at https://firebase.google.com/docs/ios/setup; "Add Firebase to your Android project," Google, available at https://firebase.google.com/docs/android/setup.

[15] "Google AdMob > Mobile Ads SDK (iOS): Get Started", Google, available at https://developers.google.com/admob/ios/quick-start; Google AdMob > Mobile Ads SDK (Android): Get Started," Google, available at https://developers.google.com/admob/android/quick-start.

[16] "Use Firebase with Google AdMob," Google, available at https://firebase.google.com/docs/admob.

[17] "Google Account," Google, available at https://www.google.com/account/about/.

[18] "Google Account," Google, available at https://www.google.com/account/about/.

web properties such as Chrome or Google Maps to the user's Google Account for the purpose of improving and personalizing user experience.

27. The WAA control includes a ***supplemental subsetting (sWAA),*** which (when enabled) allows Google to save a user's activity on third-party websites and apps that use Google services for advertising and analytics to the user's Google Accounts for personalization and improving the overall user experience.

28. Analytics SDKs, including those at the center of this litigation, often employ ***unique identifiers***, essentially a string of characters, to distinguish individual users or devices. Unique identifiers can help app developers understand how users interact with their app, identify patterns, improve user engagement, and enhance the overall user experience.

29. Unique identifiers can be tied to a user's digital identity or pseudonymized. For example, when users have enabled the WAA and sWAA settings, their web and app interactions are saved to their ***Google Account ID, known as a GAIA ID,*** a unique identifier assigned to each Google Account.

30. On the other hand, pseudonymous identifiers are designed to protect personalization preferences by not revealing the identity of the user.

31. The ***Google Advertising ID, or AdID***, is a pseudonymous identifier for Android devices. It is a unique, device-specific string of numbers and letters that is not tied to a user's identity or used to personally identify a user; users may reset their device's AdID.

32. The ***IDFA, or Identifier for Advertisers***, is the equivalent identifier for Apple iOS devices to AdID.

33. When a user signs into a Google Account on an Android phone and subsequently engages with a Google Analytics for Firebase-enabled app, in order to check the user's signed-in

account's sWAA setting, Google uses something called ***DSID, or DoubleClick ID.*** The DSID is an encrypted version of the user's GAIA ID. As described below, Google uses DSID to ensure that the true GAIA ID on the one hand and pseudonymized data tied to, for example, ADID on the other hand are never held by the same server at Google.

34. For iOS users, Google employs several methods to determine whether a user interacting with a Google Analytics for Firebase-enabled app has paused sWAA in their Google Accounts. These processes vary based on context.

35. Apple introduced iOS 14, an update to its iOS mobile operating system, in September 2020. With iOS 14, Apple released a feature called ***"App Tracking Transparency," or ATT***. This feature requires apps to request user permission before accessing the device's IDFA. If a user denies permission to an ATT prompt, the app will not be able to access the IDFA.

III. SYNOPSIS OF HOCHMAN'S EXPERT REPORT

36. Mr. Hochman is Plaintiffs' technology expert.[19] His report focuses on Google's Firebase SDK and Google Mobile Ads SDK, tools that third-party developers use to measure mobile app activity, as well as the the Web and App Activity (WAA) and supplemental Web and App Activity (sWAA) controls available to Google account holders.[20]

A. Key Technologies and Services

1. *Background*

37. Mr. Hochman first offers a "Background" into various technologies and products offered by Google. He starts with Google Accounts. Mr. Hochman correctly explains that Google allows its users to create Google Accounts, and that account–level information is

[19] Hochman Report, ¶ 9.
[20] Hochman Report, ¶ 9.

associated with an internal GAIA ID.[21] Mr. Hochman also describes that in addition to consumer Google Accounts, there are enterprise accounts (internally called "Dasher" accounts) and parent-managed accounts for children under 13 (internally called "Unicorn" accounts).[22]

38. I do not agree with any direct or indirect assertion that data practices as to "Dasher" and "Unicorn" accounts can be assessed the same as consumer accounts. These accounts are heterogeneous as to their available features and controls, which at least for "Dasher" accounts, can be tailored for organizational needs.

39. I also disagree with Mr. Hochman's assertion that identifiers like DSID, ADID, IDFA, and app instance id are "connected with a GAIA ID."[23] Google never associates these identifiers with a GAIA ID.

40. I further disagree with the assertion that "if an iOS user is signed into the Gmail app, then that user is considered 'signed in' to Google for all purposes."[24] As discussed above, Google's understanding of whether a user has signed into their Google Accounts varies based on the version of operating system and whether users have agreed to Apple's ATT setting. For iOS devices running iOS 14 or later, as I will discuss below, Google cannot determine the user's signed-in Google Account's sWAA setting.

41. Mr. Hochman then discusses the WAA and sWAA controls. He correctly describes the functions of both settings, offers their privacy policies, and explains that users are unlikely to change these settings, claiming that over a 28-day period, 99.5% of Google accounts had not modified their WAA status.[25] I disagree with Mr. Hochman's assessment that the sWAA

[21] Hochman Report, ¶¶ 37,38.
[22] Hochman Report, ¶ 39.
[23] Hochman Report, ¶ 38.
[24] Hochman Report, ¶ 40.
[25] Hochman Report, ¶¶ 40–47.

setting is "device-level," or that Google refers to this setting as "Supplemental Web & App Activity Device Level (sWAAdl)."[26] I similarly disagree with Mr. Hochman's implication that a user's ability to modify account-level controls via an Android device means that these adjustments affect device-level settings rather than account-level ones.[27] Mr. Hochman contradicts this implication soon after proposing it. He correctly notes that "WAA and sWAA are account settings that can be turned on or off across multiple devices."[28] And he adds that "a user's WAA and sWAA statuses are applied across all devices on which the user is signed-in to the same Google account."[29]

42. Mr. Hochman's subsection on WAA and sWAA also claims that, to gain regulatory approval of DoubleClick in 2008, "Google designed its display ads architecture not to link GAIA ID to data associated with display ads."[30] Mr. Hochman describes this "design decision" as "costly."[31] I do not have the expertise to opine as to whether this purported "decision" was "costly." I understand that this case primarily focuses on when Google associates GAIA ID with data from its app analytics and ads SDKs installed by third-party apps, rather than whether it links GAIA ID to its display ads business when users have consented to it.

43. Finally, I disagree with Mr. Hochman's explanation of an internal project called "Narnia 2.0," which he mischaracterizes as an "effort to link" display ads datasets with GAIA IDs.[32] "Narnia 2.0" was a multi-pronged project that sought to streamline various privacy and personalization settings. One facet of the project introduced a new "consent flow," which

[26] Hochman Report, ¶ 42; GOOG-RDGZ-00205621 at -624-625.
[27] Hochman Report, ¶ 47.
[28] Hochman Report, ¶ 50.
[29] Hochman Report, ¶ 50.
[30] Hochman Report, ¶ 54.
[31] Hochman Report, ¶ 54.
[32] Hochman Report, ¶ 54.

reminded users about their Account's activity controls and explained how they functioned. Narnia 2.0 also introduced the "My Activity" page, which provided users with a central place for users to see, manage, and delete the activity saved to their Google accounts. Additionally, the Narnia 2.0 project included the introduction of a new control called "Google Ads Personalization," or "GAP." GAP allows users to tailor the ads they see based on the web and app activity data saved to their accounts. So, whereas the WAA function influences what data is saved to a user's Google Account, the GAP function grants users the ability to choose how that data set influences the ads they see, if at all.

44. Mr. Hochman then turns to Firebase, explaining that it's an "app development platform," under which app developers install Google's Firebase SDK in order to access a range of features for building and managing an app.[33] He explains that Firebase offers Analytics features, through Google Analytics for Firebase and describes a variety of its analytics functionalities.[34] I understand that Google Analytics for Firebase is just one app analytics solution offered in a competitive field that includes offerings from Kochava, AppsFlyer, and Branch among others. I further understand that each product offers unique strengths, and that many apps utilize multiple app analytic products to leverage the strengths of each platform.

45. Mr. Hochman also discusses other Firebase products including "Predictions," "App Indexing," "Dynamic Links," and "Cloud Messaging."[35] I am not aware of any allegations that these Firebase products improperly collected sWAA-off data.

[33] Hochman Report, ¶¶ 59, 60.
[34] Hochman Report, ¶¶ 62-64.
[35] Hochman Report, ¶¶ 65-68.

46. Mr. Hochman then describes AdMob, which was "Google's solution for serving ads within mobile apps."[36] Mr. Hochman describes a number of AdMob's features.[37] Of relevance here, Mr. Hochman explains that Google integrated the Google Analytics for Firebase capabilities into AdMob's GMA SDK, so that AdMob customers could gain "a better understanding of how . . . users and ads were performing inside their app[.]"[38]

47. Finally, Mr. Hochman describes "webviews," which is a component of an app's user interface that can be used to display web pages within the app with limited web browsing. As Mr. Hochman explains, Google analyzes app interactions within webviews, but takes care to ensure that webview activity is treated the same as any other app activity and is processed through Google Analytics for Firebase.

2. *Opinions*

48. After providing background, Mr. Hochman offers his opinions. The upshot of his opinions is that Google uses various analytics and advertising products to collect[39] and save[40] data from users who had paused their WAA and sWAA settings, and then subsequently links what he calls "WAA-off" and "sWAA-off" data back to users even though they had turned sWAA off. Mr. Hochman claims that users have no way of controlling or deleting this data and that app developers have no way of preventing these practices from occurring. This data, Mr. Hochman claims, is monetized by Google. To remediate these alleged harms, Mr. Hochman claims that Google could "change WAA or sWAA to function as described," and/or "purge its systems of WAA-off or sWAA-off data."

---

[36] Hochman Report, ¶ 69.
[37] Hochman Report, ¶¶ 70,71.
[38] Hochman Report, ¶ 72.
[39] Hochman Report, ¶ 81.
[40] Hochman Report, ¶ 136.

IV. SUMMARY OF OPINIONS

A. Mr. Hochman's report does not supply a factual basis to support Plaintiffs' central allegations concerning Google's technology and its use of sWAA-off data.

49. Plaintiffs' central allegation is that Google improperly collects, saves, and profits from data from users who have paused their Account's sWAA toggle. Mr. Hochman's report does not support this central allegation and, in many instances, *disproves* the allegation. Further, Mr. Hochman relies on convenient (but baseless) assumptions, faulty methodology, and inflammatory language.

1. Contrary to Plaintiffs' allegation, Google does not intercept sWAA-off communications.

50. Plaintiffs allege that Google uses the Firebase SDK to "intercept" communications[41] between "app users on the one hand and, on the other hand, the app and the persons and entities who maintain the app (typically, the app's owners and developers), by overriding device and account level controls" such as "WAA and/or sWAA[.]"[42] To do so, Plaintiffs claim that Google "intercepts" the "communications while the same are in transit and simultaneously sends surreptitious copies of them to Google even when the user switches the Web & App Activity feature off." Plaintiffs claim that Google therefore *must* "overrid[e] device level settings, because the devices ultimately transmit and receive data, sitting between the user using the app, and the app server in the mobile cloud."[43]

---

[41] Plaintiffs define "communications" as including "who the user is," "where the user is physically located," "what content the user has requested from the app[,]" "what content the user has viewed on the app," and "much other information relating to the user's interaction with the app[.]" Complaint, ¶ 44. Most of these categories are too vague to understand the extent to which they would or wouldn't include pseudonymous information. And I do not know what Plaintiffs mean by "much other information." And, of course, much of these categories of information are not actually communications.

[42] Complaint, ¶ 43.

[43] Complaint , ¶ *45.*

51. Plaintiffs' theory is nonsensical. First, it's based on an illusory "device level setting" that does not exist. sWAA is an account-level activity control. It allows users to manage whether third-party app activity is saved to their Google Account. The fact that users can log into their Accounts with an Android device does not morph the account-level personalization controls into device-level controls. Indeed, users can log into multiple Google Accounts, each with Activity Controls, on a single Android device. A user who uses different accounts for different apps is not changing, or "overriding" the device's code each time they switch apps. The difference instead pertains to the user's Account and whether the app interaction gets saved to the account.

52. Plaintiffs' allegations also misrepresent the fundamentals of how SDKs like the Firebase SDK function.[44] App developers install SDKs; Google does not choose whether to incorporate an SDK into a third-party app. Mr. Hochman sidestepped clearly defining the term "SDK." He offered a vague definition in a footnote, stating that an "SDK, or Software Development Kit is a group of tools, including pieces of code, that are embedded into a service."[45] He notably overlooks who it is that "embeds" the SDK "into a service." It is not Google, but rather Google's customers, who have entered agreements to send data to Google.

53. While app developers choose whether or not to install an SDK, Google mandates that these developers disclose any use of its analytics SDKs, including the Firebase and Google Mobile Ads SDKs, to the users of their apps.[46] Consequently, by accepting the app's terms of service, app users have agreed to Google receiving their data for analytics services.

---

[44] *See, e.g.*, "What is an SDK?," Red Hat, available at https://www.redhat.com/en/topics/cloud-native-apps/what-is-SDK

[45] Hochman Report, fn.42.

[46] *See* Google Analytics Terms of Service, Google, https://marketingplatform.google.com/about/analytics/terms/us/ (last visited May 30, 2023) ("You must post a Privacy Policy and that Privacy Policy must provide notice of Your use of cookies, identifiers for

54. Finally, Mr. Hochman does not opine that any "interception" occurs at a technical level; that is, that Google intercepts a communication while it is in transit. I agree that this is not how the Firebase and GMA SDKs operate.

2. Contrary to Plaintiffs' allegation, Google does not personalize advertising using sWAA-off data.

55. Plaintiffs allege that Google personalizes advertising using sWAA-off data.[47] Google doesn't: a fact that Mr. Hochman effectively concedes. His report summarizes Google's practices regarding the use of sWAA for ad personalization: When a user has sWAA-on, Google saves "Chrome browsing history and activity from websites and apps that use Google services."[48] This activity data is stored in a database called "Footprints," which is described to be "the primary, canonical storage for all Google activity data."[49] "All activity-based personalization must be done using Footprints (or other primary sources like Location History), and not other data sources[.]"[50] "Google's policy is not to log sWAA-off data to Footprints[.]"[51]

56. Mr. Hochman clearly acknowledges that sWAA-off data is not used to personalize advertisements: "Google does not use data collected by GA4F from WAA- and sWAA-off users to serve personalized ads[.]"[52]

---

mobile devices (e.g., Android Advertising Identifier or Advertising Identifier for iOS) or similar technology used to collect data. You must disclose the use of Google Analytics, and how it collects and processes data. This can be done by displaying a prominent link to the site "How Google uses information from sites or apps that use our services", (located at www.google.com/policies/privacy/partners/, or any other URL that Google may provide from time to time). You will use commercially reasonable efforts to ensure that a User is provided with clear and comprehensive information about, and consents to, the storing and accessing of cookies or other information on the User's device where such activity occurs in connection with the Service and where providing such information and obtaining such consent is required by law.").

[47] Complaint, ¶ 143.

[48] Hochman Report, ¶ 143 (citing GOOG-RDGZ-00025637 at -639).

[49] Hochman Report, ¶142 & n.110 (citing GOOG-RDGZ-00118124).

[50] Hochman Report, fn. 110.

[51] Hochman Report, ¶ 144.

[52] Hochman Report, ¶ 278.

57. Mr. Hochman insinuates that Google might still "target" ads to users based on information unrelated to a signed-in user's Google account's web and app activity, such as language, device type, or the content of a website or app used by a signed-out device.[53] Even though none of these categories consist of user's signed-in app activity, Mr. Hochman inexplicably refers to them as "WAA-off" or "sWAA-off" data.[54] But "WAA" and "sWAA" are simply toggles to save data within a user's Google Account to personalize experiences based on that user's activity. In this context, the data Mr. Hochman refers to is simply regular, non-personalized data, with no relation to a user's signed-in app activity. Nothing in Google's representations on the WAA or sWAA toggles indicates a promise not to use *any* data source for what is referred to by Google as contextual ad targeting when users choose to opt out of WAA or sWAA.[55]

3. Mr. Hochman does not identify any instance of a data breach or similar event demonstrating misuse, mishandling, or abuse of sWAA-off data.

58. Mr. Hochman offers no evidence indicating misuse, mishandling, or abuse of sWAA-off data by Google or its employees, nor evidence of any breach of the agreement preventing the saving of sWAA-off data into users' Google Accounts. Mr. Hochman instead uses out-of-context documents to argue, wrongly, that "WAA-off and sWAA-off data is linked to

---

[53] Hochman Report ¶ 273.
[54] *See generally* Hochman Report ¶¶ 270-278.
[55] "How personalized ads work," My Ad Center Help, Google, https://support.google.com/My-Ad-Center-Help/answer/12155656?hl=en&co=GENIE.Platform%3DAndroid#zippy=%2Cnon-personalized-ads-on-google%2Cpersonalized-ads-on-google (last visited May 30, 2023) (distinguishing "Personalized ads on partner sites and apps," which "might be based" on information a user provides an app, a users app interactions, and Google Account activity and settings, and "Non-personalized ads on partner sites and apps," which "are shown to you according to factors like the time of day, the topic of the website you're visiting, or your general location.").

users."[56] None of Mr. Hochman's bases for this opinion appear to actually support that contention.

59. Mr. Hochman relies on the hypothetical potential for misuse over any actual examples of misuse. For instance, he outlines how Google employs pseudonymous identifiers like IDFA, AdID, and DSID to measure conversions.[57] Mr. Hochman faults these identifiers because they are unique identifiers, and theoretically (and contrary to Google policy), data associated with those identifiers could be cross-referenced against data associated with a user's Google account.[58] But Mr. Hochman does not identify any evidence that this has ever occurred. Mr. Hochman also ignores that Google maintains strong "Fingerprinting Policies" that prevent linking pseudonymous identifiers with non-pseudonymous identifiers,[59] and has implemented policies to limit employee access to logs containing pseudonymous data, including through encryption methods.

4. Mr. Hochman's use of inflammatory, biased, and colorful language in making sweeping pronouncements about the technology field or Google in particular are unsupported.

60. Throughout his report, Mr. Hochman makes sweeping and suggestive statements about either the technology field or about Google. These statements aren't expert analysis. They also are unsupported by any scientific methodology or evidence. A few notable examples are listed below.

a. "As people spend more and more time on mobile apps, those spaces have grown infested with code that tracks their every move and monetizes their data."[60]

---

[56] Hochman Report, at ¶ 301.
[57] Hochman Report, at ¶ 309.
[58] Hochman Report, at ¶ 310.
[59] *See* Appendix X4, Google's Fingerprinting Policies, and accompanying exhibits.
[60] Hochman Report, ¶ 1.

b. "Google, the dominant mobile app advertiser and collector of mobile app activity data in the United States."[61]

c. "Google has spread its code to virtually every person's phone, with Google tracking and saving vast volumes of information from hundreds of millions of Americans' app activity."[62]

d. "[T]he WAA and sWAA settings are privacy theater . . .[63] Privacy theater is described as something marketed as a step forward for consumer privacy, [that] does very little to change the underlying dynamics of an industry built on surveillance-based behavioral advertising."[64]

e. "To top it off, Google saves this WAA- and sWAA-off data (collected via the Firebase and Google Mobile Ads SDKs) in so many places, and uses it in so many ways, that even Google seems to have lost track."[65]

f. "As a practical matter, a significant number of people have no real choice whether to have a Google account. They must have a Google account."[66]

g. "Because of My Activity, Google was able to focus press and regulator attention "on the transparency improvements" and convince them that Narnia 2.0 "was a privacy positive change," notwithstanding the changes to the way Google collected and stored user data (GOOG-RDGZ-00019095 at -099 and -100)."[67]

---

[61] Hochman Report, ¶ 2.
[62] Hochman Report, ¶ 2.
[63] Hochman Report, ¶ 5
[64] Hochman Report, fn. 11
[65] Hochman Report, ¶ 5
[66] Hochman Report, ¶ 39
[67] Hochman Report, ¶ 56

h. "Google can pull the wool over its users' eyes, leaving them unaware that Google collects and saves their app activity data even when they have turned off WAA and sWAA."[68]

i. "Google in this case has relied on the relationship between app developers and users to try to excuse the fact that Google offers no way for users to delete WAA-off and sWAA-off data."[69]

B. Mr. Hochman's descriptions and opinions concerning Google's collection and saving of sWAA-off data are inaccurate.

1. Collection on Android and iOS

61. Mr. Hochman opines in his opinion A of Section VII of his report that Google "has collected WAA-off and sWAA-off data throughout the class period."[70] This opinion is peppered with further assertions regarding how Google uses the data, but his main opinions about usage of sWAA-off data come later in his report. I will address that aspect of his opinions later in this report.

62. The main point of Mr. Hochman's Opinion A is that Google Analytics for Firebase functions as designed vis-a-vis the app developer's data even when a Google account holder who has sWAA-off uses that app developer's app. In other words, the sWAA control does not change whether or not Google provides its analytics service to third party app developers. On this, Mr. Hochman and I agree. The Google Analytics for Firebase SDK is designed to help app developers understand how their users engage with their app with aggregated metrics such as

[68] Hochman Report, ¶ 144.
[69] Hochman Report, ¶ 255
[70] Hochman Report, ¶ 81.

time spent on particular articles or the geographic distribution of an app's users. This is all publicly documented functionality.[71]

63. Subject to other technical caveats not relevant here, when a GA4F user is also a Google account holder and Google has a way of checking to see that the account holder has sWAA turned off, the GA4F data the user generates is sent to Google and logged by Google in pseudonymous form on the app developer's behalf subject to the terms of use between Google and the app developer.[72] As described elsewhere herein, because the account holder had sWAA off and Google has a way of knowing that, it will not use the data to augment any marketing profile on that user, and therefore not use the data for targeting the user with particular advertising or personalizing the user's experience on Google products or services, in accordance with the WAA and sWAA control descriptions, which explain that the feature is meant to permit Google to save activity data to a user's account to use it for personalization.[73]

64. Mr. Hochman defines "WAA-off data" for purposes of his report as meaning "data generated during a user's interaction with a non-Google mobile app while that user is signed into a Google account and her WAA toggle was set to 'off'".[74] He defines sWAA-off data

---

[71] *See* Google, Google Analytics, Firebase, https://firebase.google.com/docs/analytics ("Google Analytics helps you understand how people use your web, Apple, or Android app. The SDK automatically captures a number of events and user properties and also allows you to define your own custom events to measure the things that uniquely matter to your business.").Google Analytics helps you understand how people use your web, Apple, or Android app. The SDK automatically captures a number of events and user properties and also allows you to define your own custom events to measure the things that uniquely matter to your business.").

[72] *E.g.*, Google's Supplemental Responses & Objections to Plaintiffs' Interrogatories, Set 7 ("Interrogatory Response, Set 7"), Interrogatory No. 23, at p. 18 ("When a user is logged into their Google Account and has turned WAA and/or sWAA off, any data that is collected by the Google Mobile Ads SDK is logged against pseudonymous identifiers."); *see also* Langner Tr. 185:13-17 ("For Google Analytics for Firebase data, when the user has sWAA-off, the Google Ads systems can use data in this pseudonymous space for the purposes of conversion measurement[.]").

[73] ROG 1, p. 23-26; Ganem Depo 68:21 -74:5; Hochman Report, ¶¶166, 250.

[74] Hochman Report, ¶ 82.

as the equivalent, but for sWAA toggled to off.[75] This is a confusing way to define these terms because it is not limited to the products at issue — the GA4F SDK, the GMA SDK (encompassing AdMob and AdManager), and Firebase Cloud Messaging. It is also not narrowed to include only data sent to Google along with sufficient information for Google to determine the user's identity for purposes of checking the user's privacy control settings. Mr. Hochman repeatedly concedes that Google cannot honor a privacy control for an account it can't identify. For this reason, where in his definition he mentions the user being "signed into a Google account," I will interpret that to be a shorthand for situations where Google can identify the user on Android or iOS sufficiently to determine the user's sWAA setting status. Finally, his definition implies that *all* data generated by virtue of the user's use of the app constitutes at-issue data, but it does not. The WAA control applies only to "web & app activity data," and so only app activity data should be included in the data subject to the use of a term like "WAA-off data."

65. With those caveats and narrowings, I will refer to the at-issue data as sWAA-off analytics, sWAA-off GMA, and sWAA-off FCM data, collectively: sWAA-off data. I will explain further below which data constitute, in my opinion, activity data, and which cannot, as a technical matter, be considered activity data. For the most part, once the technical details have been taken into account, it is fair to say Mr. Hochman and I generally agree on the scope of at-issue data.

66. I understand from Mr. Hochman's report that he limits his technical opinions in this case to U.S. Google account-holders who were neither "unicorns" (under 13 years of age) nor whose accounts were enterprise or government accounts ("dasher," etc.), *i.e.*, Plaintiffs' claims and Mr. Hochman's opinions are limited to end users of mobile apps on Android or iOS

[75] Hochman Report, ¶ 83.

with Google accounts who were not under thirteen years of age and whose accounts were set up by that user as a standard consumer account, which Mr. Hochman also refers to as "consumer accounts."[76]

a. Google Analytics for Firebase

67. Mr. Hochman opines that "WAA and sWAA settings have no impact on the types of data collected by Google app analytics products."[77] As to GA4F and the analytics products incorporated into the GMA SDK, Mr. Hochman is partially correct. Throughout his report, Mr. Hochman mixes the concepts of collection, saving, and using. For example, in the next sentence, he discusses collection and saving in the same sentence. This conflation makes it difficult as a technical matter to opine accurately about Google's technology. In this report, I will carefully separate those concepts.

68. The types of app activity data sent to Google by apps that use GA4F and the GMA SDK are the same regardless of the user's account-level sWAA setting: they are the app activity data the app developer has requested Google collect for their analysis of their own apps and the way users use them. The infrastructure supporting the collection of data in GA4F and GMA SDK are the same.[78] As a result, in this report, whenever I refer to GA4F analytics functionality, that applies equally to the analytics functionality incorporated into the GMA SDK.

69. How the data sets are saved and used by Google differ depending on the user's sWAA setting. The app activity data sent to Google by GA4F is described in Google's interrogatory responses and in Mr. Hochman's report. It is also publicly documented by Google in its Firebase help center pages. At a high level, as Mr. Hochman describes, GA4F logs events

[76] *See e.g.*, Hochman Report, ¶ 39
[77] Hochman Report, ¶ 87.
[78] Google LLC's Fourth Supplemental Responses and Objections to Plaintiffs' Interrogatories Set One, Interrogatory No. 3, at 46.

to the user's device (either to a central log on Android or to an app-specific log on iOS), and those logged events are later uploaded to Google servers for consent checks, processing, and saving. On this, Mr. Hochman and I agree.

70. Standard GA4F events are, as Mr. Hochman describes, items like "first open." Google lists the current automatically collected events by GA4F on its Google Firebase support documentation.[79] These events are logged by GA4F with accompanying information; Mr. Hochman's report contains samples of the information first collected by GA4F at Hochman Appendix H.1 and H.2, and complete data productions of those initial collection logs as they pertain to Mr. Hochman's test devices were produced at GOOG-RDGZ-20833 and -834.

71. The way GA4F events are logged implies that an event occurred, but does not necessarily imply anything in particular about that event. For example, the "first_open" event is triggered "the first time a user launches an app after installing or re-installing it," and stored with that event is the device information (*e.g.*, ADID or IDFA, resolution, device type, etc.) and a timestamp.[80] The way GA4F logs this event does not contain any information about what the user saw or did on the app; only that the user opened the app at the given time. Another example: the event "screen_view" indicates that the app loaded a particular screen of the app at a given time.[81]

72. It is important to realize that how these events are customized is up to the app developer, and app developers can also create custom events of their own. Mr. Hochman does not acknowledge in his report that event parameters designed by an app developer may mean

---

[79] "[GA4] Automatically collected events", Analytics help, available at https://support.google.com/analytics/answer/9234069?hl=en.
[80] "[GA4] Automatically collected events", Analytics help, available at https://support.google.com/analytics/answer/9234069?hl=en.
[81] "[GA4] Automatically collected events", Analytics help, available at https://support.google.com/analytics/answer/9234069?hl=en.

something to that app developer, but not to Google. For example, one of the "page_view" parameters is "page_location," which is filled in dynamically by the GA4F SDK with the page URL. The exact URL of a page in an app may mean something to the app developer, but it means nothing to Google, and Mr. Hochman does not identify any evidence in his report suggesting otherwise, nor does he suggest that Google makes use of the page URL information for any purpose. As far as I am aware from my review of the evidence I've been provided, Google does not do so.

73. Nor would it make sense to do so— each app could have thousands of page locations, and there are over a million apps that use Firebase. It would be practically impossible for Google to decipher what every page_view means. As discussed later in this report, Google can make use of the fact of a page_view as indicating user engagement of some kind, but it cannot know exactly what the user was looking at. And, as discussed later, Google only does this when it knows that sWAA is on or when Google cannot know a user's account settings because the user is signed out of any Google account. Likewise, when the "in_app_purchase event" is triggered, information about which product was purchased and how much it cost is recorded, but the product_id will mean something only to the app developer, not to Google. At most, Google is able to know that an in-app purchase occurred and how much was spent, but not exactly what was purchased. Mr. Hochman's report does not suggest otherwise, nor have I seen any evidence suggesting that Google is able to and does decipher product_ids in this way. And, of course, even if it could, it does not use such data if it is sWAA-off data.

74. Along with events sent to Google by apps that use GA4F, there are also "user properties" that come with the data sets. These user properties can include demographic information about the user, but only if the app developer has set that information. As Google's

public documentation explains, an app developer can set a variety of user properties. For example, Google tells app developers: "you can set a user property called favorite_food, which you can use to record each user's favorite food. You can use the data to segment users by their favorite food."[82] Some user properties are automatically filled in by GA4F if the information is available to it.[83] The degree to which such information is available varies widely, and also varies depending on the app developer and user privacy settings. This is evident in the data Google produced about the named Plaintiffs. Out of 123,302 events logged in those data sets, 49% had no age information,[84] 49% had no gender information, and 59% had no information about the user's interests.[85] 100% had coarse geographic information derived from IP addresses. The IP addresses themselves are not logged or stored, per Google's policies.[86]

---

[82] "[GA4] Users properties", Analytics help, available at https://support.google.com/analytics/answer/9355671?hl=en.

[83] "[GA4] Predefined user dimensions", Analytics help, available at https://support.google.com/analytics/answer/9268042.

[84] Strangely for Mr. Rodriguez's 53,167 event entries (based on his ADID), 40,293 (76%) had age unknown while 12,447 (23%) had age range 18-24 and 427 (1%) had age range 35-44. *See* GOOG-RDGZ-00071766 and GOOG-RDGZ-00071767.

[85] Mr. Hochman suggests that "potentially even favorite food" could be recorded in the baseview log. Hochman Report, ¶ 89. But Mr. Hochman took this from a Google page giving examples of what user_properties a developer could collect from users, not what something that Google automatically records; in the instant baseview log there were zero entries regarding foods. *See* [GA4] Automatically Collected Events, Google Analytics Help, https://support.google.com/analytics/answer/9234069?hl=en (Last visited May 30, 2023). Nor does an app developer's decision to log for itself a user's favorite food necessarily mean that Google would use that information for any other purpose.

[86] "Prepare for the future with Google Analytics 4," Google, available at https://blog.google/products/marketingplatform/analytics/prepare-for-future-with-google-analytics-4/ ("Google Analytics 4 will also no longer store IP addresses.");"EU-focused data and privacy," Google, available at https://support.google.com/analytics/answer/12017362?hl=en#:~:text=Google%20Analytics%204%20does%20not%20log%20or%20store%20individual%20IP,and%20ID%2Dbased%20counterparts. Although this webpage is titled "EU-focused data and privacy, I understand that it is describing how Google Analytics works regardless of location. I have also personally reviewed the logs produced by Google and have not found IP addresses in them. Nor did Mr. Hochman.

75. These statistics are not surprising. As Mr. Hochman explains, one way Google provides app developers with demographic information about the users of their apps that have GA4F enabled is by relying on Google Signals, a feature that app developers must opt into. According to Google's support pages, "Google signals are session data from sites and apps that Google associates with users who have signed in to their Google accounts, and who have turned on Ads Personalization. This association of data with these signed-in users is used to enable cross-device reporting, cross-device remarketing, and cross-device conversion export to Google Ads."[87]

76. Thus, if the app developer opts in and if the user has sWAA and Google Ads Personalization turned on, Google can supply the app developer with richer information about the user for their own analysis. But this only works if the user has sWAA on; if the user has sWAA off, this demographic information associated with the user's Google account is not looked up by Google, and not provided to the app developer.[88]

i. Mr. Hochman misrepresents the collection of identifiers by the analytics products.

77. Although his basic technical discussion of GA4F app activity data is fairly accurate, in his discussion of "identifiers" sent to Google with GA4F data, Mr. Hochman makes a multitude of errors describing what data are sent to Google.[89]

78. First, Mr. Hochman asserts that "One of the identifiers that Google collects and saves via GA4F is the GAIA ID, which is unique to the user's Google account. Google collects

[87] "[GA4] Activate Google signals for Google Analytics 4 properties,"Analytics help, available at https://support.google.com/analytics/answer/9445345#zippy=%2Cin-this-article%2Cdemographics-and-interests.
[88] Ganem Depo. 256:11-24.
[89] *See* Hochman Report,¶¶ 100-113.

the user's GAIA ID regardless of their WAA or sWAA status."[90] None of that is correct. As Mr. Hochman later acknowledges, on Android, GA4F sends a DSID to Google, not a GAIA ID. The DSID is "an encrypted version of the user's GAIA ID."[91] The DSID is used on Google's end to check the user's sWAA setting and other privacy settings.[92] I will discuss the consent check process in more detail below, but as Mr. Hochman himself explains, the DSID is sent by the analytics server to a separate server, and the separate server decrypts it, determines the user's settings, and reports the settings back to the analytics server, thereby ensuring that the true GAIA ID on the one hand and the ADID and analytics data on the other hand are never held by the same server at Google until it is confirmed that the privacy controls of that user would permit it.[93] Thus, it is plainly incorrect that "One of the identifiers that Google collects and saves via GA4F is the GAIA ID," as Mr. Hochman claims in paragraph 101 of his report. GA4F does not collect the GAIA ID, and Google does not save it. Nor is the analytics data ever intermixed with the GAIA ID unless it is first confirmed that the user's privacy controls would permit it, including that sWAA is on.

79. As for iOS, the GAIA ID is not sent with the GA4F hit bundles at all. As Mr. Hochman explains, only IDFA is sent, which is a device ID. On Google's end, if it is able, according to the process laid out below, Google determines whether that IDFA is associated with a GAIA ID, and if so, what the privacy settings are so that it may honor those settings.[94]

80. Second, Mr. Hochman cites GOOG-RDGZ-00207704 as support for his claim that "Google's internal document explains that 'through its association with Android ID and

---

[90] Hochman Report,¶ 101.
[91] Hochman Report,¶ 162.
[92] Hochman Report,¶ 163.
[93] Hochman Report, ¶ 163.
[94] *See* Hochman Report, ¶ 164.

GServices AID, IID (which is unique per app-device combination) can be mapped to GAIA on Google's backend.'"[95] The source document for this claim does not support Mr. Hochman's implication that because it could theoretically be mapped, it is. Instead, the document explains in the next sentence that "None of the features in this proposal depend on or leverage this association in any way." GOOG-RDGZ-00207704 at -705. And in the next paragraph, the document further explains that "A significant amount of work has been done recently to separate access to this mapping, and to institute access controls so that Googlers cannot perform this mapping." *Id.* The rest of the document describes several options for Google to pursue to ensure that a GAIA mapping does not become possible. Mr. Hochman does not cite any evidence indicating which option Google ultimately adopted. I am not aware of any evidence that Google chose to pursue any option that uses or leverages a mapping between IID and GAIA. To the contrary, Mr. Ganem in his deposition, confirmed that IID is not saved at all unless users consent to sWAA and GAP.[96]

81. Third, Mr. Hochman notes that app developers can assign users a "User ID" unique to that user.[97] I agree this is a feature of GA4F. But to the extent Mr. Hochman is implying that this somehow results in Google tying data to a particular user for its own purposes, I disagree. There is no evidence of which I am aware that Google uses "User ID" as defined by an app developer to do anything. App developers can choose to assign these unique User IDs, and use them for their own purposes.

82. Fourth, and more generally, in this section of his report, Mr. Hochman seems to take issue with the fact that there are "dozens upon dozens of additional identifiers" involved in

[95] Hochman Report, ¶ 107.
[96] Ganem Deposition Transcript, 214:20-215:9.
[97] Hochman Report, ¶ 109.

analytics products.[98] But nowhere in his report does he demonstrate that identifiers in a pseudonymous log are matched to a user's identity such that the identifier is converted into a personally identifiable string. I have seen no evidence that Google does this with sWAA-off data, and Mr. Hochman does not identify any such evidence.

83. In this section of his report, Mr. Hochman also makes the following claim:

> Google links many of these identifiers together. Through internal mechanisms such as [redacted], and [redacted], for example, Google links IDFA and ADID to other Google identifiers, such as Zwieback (which is associated with Google Search) and Biscotti (which is associated with display ads), which, together with GAIA, enable Google's ads integrations (GOOG-RDGZ-00176250 at -250; GOOG-RDGZ-00056108 at -114, -115).

84. Hochman Report, ¶112. This is a highly misleading paragraph, and Mr. Hochman notes that he expands on his claims here later in his report. I will also address this concept in more detail later in this report, but as it pertains to this passage, Mr. Hochman fails to mention that joining of pseudonymous identifiers to each other, *e.g.*, ADID to Biscotti, does not convert the identifier into a personally identifiable one because Google maintains a strict boundary between pseudonymous identifiers on the one hand and GAIA and other PII on the other.[99] I am aware of no evidence that Google has failed to maintain that boundary, and Mr. Hochman does not cite to any. The phrase in this passage "together with GAIA, enable Google's ads integrations" is strictly true only insofar as the user has consented via turning sWAA on; Mr. Hochman fails to mention that the joining "together" of pseudonymous IDs to GAIA is otherwise

[98] Hochman Report, ¶ 110.
[99] ROG 1, at p.6

forbidden.[100] Nowhere in his report does Mr. Hochman identify any instance of Google intentionally or knowingly joining a pseudonymous ID to a GAIA ID or other PII.[101]

b. Google Mobile Ads SDK

85. Mr. Hochman opines that Google uses the GMA SDK (including Google Ad Manager, AdMob and AdMob+) to "collect and save app activity data" even when the user has sWAA turned off. Insofar as this is an opinion about Google's analytics products, my discussion above applies equally here. Insofar as Mr. Hochman is opining that ads-related data generated by the GMA SDK constitutes "app activity" data, as a purely technical matter, I disagree. As for analytics-related data, my opinions above concerning GA4F apply equally here because GA4F and the GMA SDK share the same infrastructure for analytics data.[102]

86. The ads-related data from the GMA SDK Mr. Hochman identifies are data concerning "ad events": in particular, ad requests, ad impressions, and ad clicks. Mr. Hochman assumes without opining that these ad event categories are "app activity data" within the meaning of the sWAA control. In my opinion, these ad events are not "app activity" or "user activity" data. They are merely high-level records of services Google provides to apps and

---

[100] *Id. See also* 8:2-9, 11:6-16:15.

[101] In some sections of his report, Mr. Hochman identifies anomalous analytics entries where an app developer has customized their analytics SDK to send email addresses to Google alongside pseudonymous data. This is forbidden by Google's terms, and as discussed later, is not the norm. Nothing about GA4F's design invites this or deems it permissible, and GA4F "out of the box" does not join email addresses or other PII to any pseudonymous identifier."Upload data use policy," Google Analytics Help, available at https://support.google.com/analytics/answer/2838984 (last accessed May 30, 2023) ("You will not upload any data that allows Google to personally identify an individual (such as names, social security numbers, email addresses, or any similar data), or data that permanently identifies a particular device (such as a mobile phone's unique device identifier if such an identifier cannot be reset), even in hashed form. If you upload any data that allows Google to personally identify an individual, your Google Analytics account can be terminated, and you may lose your Google Analytics data."

[102] GOOG-RDGZ-00067721, at 722.

websites that serve ads and to advertisers so that Google can engage in the necessary bookkeeping that I understand from Dr. Knittel this is standard in the advertising industry.[103]

87. Notably, Mr. Hochman's report discusses ad events only in cursory fashion, and does not identify what about them is private. Notably, Mr. Hochman identifies his Appendix K as the appendix in which he provides examples of information recorded by Google when sWAA is off that constitutes private information.[104] None of the examples given in Appendix K come from Google's adEvents log, which is what contains ad event data. Mr. Hochman provides the ad event data Google produced in his Appendix F.

88. An ad request is triggered when an app that has ad space inside it needs to request an advertisement to display in the app. "An ad request is counted each time a request is sent, even if no ads are returned and/or when house ads are shown."[105] An ad request includes information about the device requesting the ad, the app requesting the ad, and the requested format of the ad.

89. An ad impression "is counted when one or more pixels of the ad creative is visible on a device's screen."[106] Here again, the ad impression entries include information about the device displaying the ad, the app displaying the ad, and the format of the ad.

90. In his report. Mr. Hochman identifies an "ad view" as separate from ad impression, but I do not see evidence supporting that distinction. Instead, I understand from the

---

[103] Knittel Report, ¶¶ 29-35.
[104] *See* Hochman Report, ¶179 & App'x K.
[105] "Ad request", Google AdMob Help, available at https://support.google.com/admob/answer/3544753?hl=en#:~:text=When%20your%20app%20requests%20ads,when%20house%20ads%20are%20shown.
[106] "Ad request", Google AdMob Help, available at https://support.google.com/admob/answer/3269069?hl=en&ref_topic=7383088&sjid=4439213764704631058-NA.

evidence and Mr. Hochman's own report that AdView is terminology Google uses to name a log that contains ad impression data.[107]

91. An ad click is what it sounds like: a record that a user clicked (or tapped) on an ad shown in a third party app or other advertising surface, such as a website. Here again, the ad click entries in the record include information about the device displaying the ad, the app displaying the ad, and the format of the ad.

92. From my review of the adEvents log entries Google produced, I do not see any information in the entries that could be considered "app activity" information, as none of it relates to the activity the user engages in within the third party app serving the ad. The recording of ad requests, impressions, and clicks alongside device information, timestamps, and other similar record information is all directed at making a record that a user was shown or interacted with an ad, so that the advertiser whose ad it is can know that. In this way, Google serves as a bookkeeper for the advertiser. I am not aware of any use Google makes of sWAA-off adEvent data other than to calculate conversions, as Mr. Hochman describes. And that calculation simply connects the advertiser's interaction with the user at time 1 with another interaction with the same advertiser at time 2.

93. Next, Mr. Hochman opines that ad events data include identifiers. From my review of the entries Google produced and the related evidence, I agree that ad events data can include identifiers, and typically will include either a pseudonymous identifier such as ADID or IDFA (when sWAA is off) or a GAIA (when sWAA is confirmed on). These identifiers can

[107] Hochman Report, ¶ 122 (Google Mobile Ads SDK sends data to "several types of ad events," including "ad views, in which the user views an ad displayed in the app[.]").

facilitate the task of reporting to an advertiser that the same ADID that clicked on an ad at time 1 ultimately installed the advertiser's app at time 2.[108]

94. Mr. Hochman opines in connection with his opinion on the collection of data via the GMA SDK that "If Google did not collect and save ad requests, it could not serve ads."[109] It is unclear what he means here, but if he means that, to honor the sWAA control, Google would have to refuse to serve ads to confirmed sWAA-off devices through AdMob or Ad Manager, I see no evidence in the record that this is how anyone else understood the sWAA toggle. Not only is the ad events record information not app activity data, but in my opinion it would be unreasonable to assume that the sWAA toggle as described should function, in effect, as an ad blocker across apps and the Internet wherever Google serves ads.

c. Firebase Cloud Messenger

95. Mr. Hochman opines briefly that "Google collects a variety of information via Firebase Cloud Messaging, including several types of events, parameters, and user properties."[110] Here, again, Mr. Hochman does not explain how these data types are used, why they are collected, or what privacy violation Plaintiffs allege could be derived from the use of FCM by its design.

96. Indeed, I am unaware of any evidence that Google uses the FCM data Mr. Hochman describes in his Appendix I ¶ 58-62 (as evidence of sWAA-off collection of FCM

---

[108] Mr. Hochman fails to note that there is a collection toggle on Android and iOS devices that would prevent the collection of the ADID or IDFA corresponding to the mobile device: on Android, this is known as OOOAP, or Opt Out of Ad Personalization. Google's Fourth Supplemental Responses and Objections to Plaintiffs' Interrogatories Set Seven, Rog 25, p. 20. On iOS, this is known as LAT, or Limit Ad Tracking. *Id.* *See also* "Limit Ad Tracking," Singular, https://www.singular.net/glossary/limit-ad-tracking/. Since iOS 14, this has instead been known as ATT, or App Tracking Transparency. Google's Fourth Supplemental Responses and Objections to Plaintiffs' Interrogatories Set Seven, Rog 25, p. 7. In all cases, users have a device-level setting that can prevent the collection of this identifier.

[109] Hochman Report, ¶ 122.

[110] Hochman Report, ¶ 132.

data) for any purpose other than to serve analytics information to the app developer who sent the notifications. Therefore, I see no technical way in which the functioning by design of FCM could be implicated by Plaintiffs' allegations. At most, Google serves as a conduit for app developers to send notifications to their own users.

97. It is also notable that Mr. Hochman does not discuss that users must agree to receive notifications from an app on an app by app basis before an app developer can send that user a Firebase Cloud Messenger notification.[111] If Mr. Hochman's opinion is that FCM somehow violates user expectations as set up by the sWAA control, the necessary implication of that opinion would be that even when users opt into receiving notifications, if the app developer uses Firebase, the notifications will not be served to the user if the user has also turned the Google sWAA toggle to off. This is obviously nonsensical because the user has opted into receiving notifications, but because of the app developer's choice of analytics provider, that request is simply ignored.

2. Saving on Android and iOS

98. Mr. Hochman opines that "Google, throughout the class period, has uniformly saved class members' WAA-off and sWAA-off data in numerous logs. Such data is identified as belonging to particular users through the various IDs Google saves and uses."[112] His opinion is significantly inaccurate, and there are some indications it is also unreliable.

a. Google Analytics for Firebase

i. Consent Checks

[111] For Android devices, the app developer includes a request for permission to send notifications in the app's manifest which causes a dialog to appear to the user, requesting permission; *see* "Notification runtime permission", Android, available at https://developer.android.com/develop/ui/views/notifications/notification-permission

[112] Hochman Report, ¶ 136.

99. Mr. Hochman mostly characterizes the consent check process on Android for GA4F correctly. Generally speaking, and as I have already discussed, Android devices send a DSID token with analytics hit bundles from GA4F or GMA SDK which is subsequently used to determine the user's privacy settings. The DSID is not itself a GAIA ID, and the analytics server that receives it does not know to whom the DSID token belongs. Instead, the collection endpoint server sends the DSID to a separate server that decrypts it, determines the user's privacy settings, and then reports back to the analytics server whether the data can be saved alongside a GAIA ID (in which case a GAIA ID is also reported back to the analytics server) or if instead it must be saved in pseudonymous form because, *e.g.*, the user's sWAA toggle is set to off.[113] (And in this latter case, the GAIA ID is *withheld* from the analytics server.) In this manner, two separate servers are in possession of separate pieces of information–the user's identity and the analytics data–until it is confirmed whether sWAA is turned on; and the data are held in ephemeral memory while the consent check is pending.[114] This ensures that the true GAIA ID on the one hand and the ADID and analytics data on the other hand are never held by the same machine at Google until it is confirmed that the privacy controls of that user would permit it.[115]

100. The consent check process for iOS is different. Hochman opines that "Users of iOS devices are treated as 'signed in' to a Google account if they are signed in on any Google app on their device."[116] This description is incomplete. A more precise one would be asking the question of whether Apple's operating system allows Google to obtain a user's GAIA in order to look up that user's consent settings when receiving GA4F or advertising data. There are several

[113] Google LLC's Fourth Supplemental Responses and Objections to Plaintiffs' Interrogatories Set One, Rog 1, p. 12, 24.
[114] Google LLC's Fourth Supplemental Responses and Objections to Plaintiffs' Interrogatories Set One, Rog 1, p. 12, 24.
[115] Hochman Report, ¶ 163.
[116] Hochman Report, ¶ 40.

factors that will affect if Google is able to perform a GAIA lookup, and it depends on whether the lookup was being performed before or after iOS 14, which was released in September 2020.

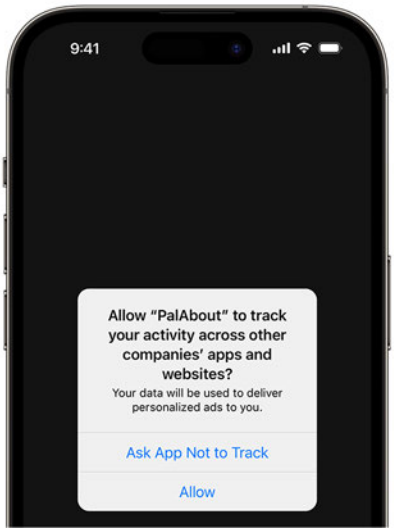
101. Before iOS 14, Google was able to log both IDFA and GAIA ID in a linking table.[117] This table was strictly controlled and used by Google solely for the purpose of performing consent checks because, technologically speaking, there were no other methods available to obtain a user's Google Account identity from iOS to determine the user's privacy settings.[118] The linking table was populated by first party Google apps, and in this manner was only partially reliable. Not all users had first party Google apps installed, and such users would not have any entries in the linking table. Further, IDFAs could change or be reset, and the accounts used to log into the first party apps could change as well, making individual entries in the linking table not necessarily accurate.[119] If no first party apps were installed on iOS and no other means were available to determine the user's identity from iOS, Google treated app activity data as pseudonymous data with an unknown sWAA setting.[120]

102. Google's efforts in this regard were intended to tie iOS user data to a user's Google identity when there was permission, and to prevent the writing of activity data to a marketing profile when the user was determined to have sWAA turned off.[121] This pro-privacy method of looking up a user's identity and determining the user's privacy control settings ended with iOS 14.

---

[117] Ganem Depo 68:21-70:19.
[118] Ganem Depo 71:5-73:4
[119] Ganem Interview May 18, 2023.
[120] Ganem Interview May 18, 2023
[121] Ganem Interview, May 18, 2023

103. With iOS 14 Apple introduced "App Tracking Transparency," or ATT.[122] Developers must implement the App Tracking Transparency framework in their iOS apps "if your app collects data about end users and shares it with other companies for purposes of tracking across apps and web sites."[123] The ATT framework issues the user a prompt when an app employing the framework is first opened asking the user whether the third party app should be allowed to "track your activity across other companies' apps and websites" or other similar language. The user can choose to allow or "ask app not to track."[124]



104. If the user clicks "ask app not to track," then "the app developer can't access the system advertising[125] identifier (IDFA), which is often used to track. The app is also not permitted to track your activity using other information that identifies you or your device, like your email address."[126]

---

[122] "App Tracking Transparency," Apple, available at https://developer.apple.com/documentation/apptrackingtransparency.
[123] "App Tracking Transparency," Apple, available at https://developer.apple.com/documentation/apptrackingtransparency.
[124] "If an app asks to track your activity," Apple, available at https://support.apple.com/en-us/HT212025.
[125] "If an app asks to track your activity," Apple, available at https://support.apple.com/en-us/HT212025.
[126] "If an app asks to track your activity," Apple, available at https://support.apple.com/en-us/HT212025.

105. By blocking access to IDFA, iOS 14 and the ATT framework prevented Google from tying a user's logged-in identity on a first party Google app to the device IDFA.[127]

106. The upshot is that users with devices post-iOS 14, Google is not able to check users' sWAA control settings from analytics data sent to Google from iOS. For this class of users, Google is completely prevented by iOS and Apple's terms and conditions from determining the iOS user's Google Account privacy settings in third party apps, such as whether they have sWAA turned on or off.

107. Mr. Hochman claims that "if the developer of a single app on a user's device enables Google Signals, that user's device ID (*i.e.*, ADID or IDFA) will be linked to their GAIA ID, creating a link that persists even for apps that do not enable Google Signals."[128] It is unclear from where Mr. Hochman got this understanding; he does not cite a source. But, as discussed throughout this report, Google does not associate analytics or ads-related data across GAIA and ADID.[129] And while Google did, before iOS 14, use both GAIA and IDFA for the purpose of checking the user's consent settings in order to honor those settings,[130] I am aware of no evidence that this link was ever used for any other purpose, which would violate Google's policies. That linking table could not be populated with new information after iOS 14.[131] In any case, the implication of Mr. Hochman's statement is that Google links ADID or IDFA to GAIA

---

[127] Ganem Interview, May 18, 2023

[128] Hochman Report, ¶ 167.

[129] Google LLC's Supplemental Objections and Responses to Plaintiffs' Interrogatories Set Six, Rog 17, p. 15 (explaining ADID and IDFA is a "pseudonymous identifier"); Google LLC's Fourth Supplemental Responses and Objections to Plaintiffs' Interrogatories Set One, Rog 1, p. 25 ("From the signed-in GAIA copy of data, Google removes all pseudonymous identifiers. From the signed-out pseudonymous log, Google removes all signed-in [i.e. GAIA] identifiers. The result is that the two logs don't overlap identifiers that could be used to join the logs together.").

[130] Ganem Depo, 68:21-73:3

[131] Ganem Depo 72:4 - 72:22. Google LLC's Supplemental Responses and Objections to Plaintiffs' Interrogatories Set Six, Rog 17, p. 15.("If the iOS IDFA is zeroed out because the user has enabled LAT or clicked "Don't Allow" on the App Tracking Transparency prompt, GA4F would be unable to directly associate app-install conversions with ad impressions and clicks which drove them.")

in order to better advertise to that user, but, as Mr. Hochman concedes, when sWAA is off, this will not happen.[132]

108. Mr. Hochman claims that "A user can also be signed out of Google. In this case, all collected data are stored with a user's non-GAIA Google identifiers. Regardless of user or app developer settings, a copy of the user's app analytics data is stored by Google in the user's Google Account."[133] The last sentence does not logically follow from the first two, and must be a typo or inadvertent error. It is not true that regardless of the user's settings, a copy of app analytics data is stored "in the user's Google Account." As Mr. Hochman repeatedly concedes, this is not true when the user's sWAA is turned off, and when the user is signed out and an identity cannot be confirmed, by definition the analytics data cannot be saved with the user's Google Account, as Google has no way of knowing whose Google account to save it to.[134]

109. Next, Mr. Hochman takes issue with Google's decision to check a user's sWAA setting at the server level rather than at the device level. In my opinion, Mr. Hochman's proposal that Google check the sWAA setting at the device level would not result in any change in how Google handles the analytics data sent to it by apps that use GA4F. Even if the check were performed at the device level, when sWAA is off, GA4F would still send pseudonymous data to the analytics collection endpoint, from which it would be processed for the app developer's analytics uses.

---

[132] Google LLC's Second Supplemental Responses and Objections to Plaintiffs' Interrogatories Set Six, Rog 17, p. 15.("Regardless, no data in this scenario would be written to [redacted] or used for personalized advertising"), Google LLC's Fourth Supplemental Response and Objections to Plaintiffs' Interrogatories Set 1, ROG 1, p. 23-26; Ganem Depo, 68:21 -73:3. Hochman Report, ¶¶ 166, 250

[133] Hochman Report, ¶ 170.

[134] Google LLC's Fourth Supplemental Response and Objections to Plaintiffs' Interrogatories Set 1, Interrogatory No. 1, at p. 23-26; Ganem Depo 68:21 -73:3 Hochman Report. ¶¶ 166, 250.

110. I do not understand Plaintiffs to be alleging in this case that the analytics function itself violates user privacy, and Mr. Hochman does not render such an opinion. Nor would such an opinion make sense – app developers are, of course, able to use any number of analytics services to study the interactions of their own users with their own apps; that Google is sometimes selected to provide that service does not make the user's data more or less private unless Google also subsequently uses the data for improper purposes. Since, at a minimum, the sWAA-off analytics data will be stored by Google on analytics servers to provide app developers with analytics services, the consent check can occur on device or at the server level – it makes no difference regarding privacy of user data.

111. Finally, in this section of his report, Mr. Hochman claims that Google "is . . . saving WAA-off and sWAA-off data to class members' Google Accounts."[135] This is plainly untrue, but explained by Mr. Hochman's footnote 104, in which he defines the concept of "Google Account." When stating "Google Account" he is "referring collectively" to data saved pseudonymously, *i.e.*, data not associated with a GAIA ID or with a user's email address or identity. In this manner, Mr. Hochman defines away the central question of his report—whether and how Google respects the sWAA off toggle, which is meant to give Google permission to "save" specified data "in your Google Account."[136] This sleight of hand makes me question the reliability of all of Mr. Hochman's conclusions, because he has hidden a definition, on page 65 of his report (just about halfway through the entire report) that changes the fundamental meaning of a key term in the case.

---

[135] Hochman Report, ¶ 136.

[136] *See* "My Activity," Google My Activity, available at https://myactivity.google.com.(offering users the ability to "Choose which settings," including WAA and sWAA, "will save in your Google Account").

112. Mr. Hochman also redefines the term "Google Account" to be broader than the term as defined by Google in its own policies and terms that it employs with consumers. For example, the current privacy policy defines "Google Account" in a "key terms" section as:

> You may access some of our services by signing up for a Google Account and providing us with some personal information (typically your name, email address, and a password). This account information is used to authenticate you when you access Google services and protect your account from unauthorized access by others. You can edit or delete your account at any time through your Google Account settings.[137]

113. The privacy policy goes further, and describes the difference, in Google's view, between non-personally identifiable and personally identifiable information:

> **Non-personally identifiable information**
>
> This is information that is recorded about users so that it no longer reflects or references an individually-identifiable user.
>
> **Personal information**
>
> This is information that you provide to us which personally identifies you, such as your name, email address, or billing information, or other data that can be reasonably linked to such information by Google, such as information we associate with your Google Account.[138]

114. My Appendix X6 summarizes the historical definitions of these terms as they have appeared in Google's policies with its customers and consumers for the entire class period.

---

[137] "Privacy and Terms," Google, available at https://policies.google.com/privacy/key-terms?hl=en-US#toc-terms-account.

[138] "Privacy and Terms," Google, available at https://policies.google.com/privacy/key-terms?hl=en-US#toc-terms-account.

At no time has Google ever defined "Google Account" in a manner consistent with Mr. Hochman's redefinition of the term in his report at footnote 104.

115. Leaving aside semantics, as a technical matter, Mr. Hochman concedes that he is referring to pseudonymous data when he makes statements such as these.[139] It is undisputed that the consent check process employed by Google is designed to and does separate pseudonymous data from data associated with a GAIA ID in Google's logs, as well as to prevent the writing of sWAA-off analytics data to any marketing profile used by Google Ads to personalize advertising.[140]

ii. Storage

116. In the same vein as his claim that Google saves sWAA-off data to users' Google Accounts, as he redefines that term, Mr. Hochman claims that "Google intermixes both WAA-on and sWAA-on data with WAA-off and sWAA-off data" and that "it does not appear that Google treats the WAA-off and sWAA-off data in Google's non-GAIA logs any differently than it treats the WAA- on and sWAA-on data in those logs."[141] Mr. Hochman repeats this claim later in his report.[142]. There is no factual basis for those claims.

117. First, Mr. Hochman walks through a general, high-level overview of Google's data infrastructure, none of which is tethered to Mr. Hochman's opinion regarding Google's purportedly equal treatment of sWAA-on and sWAA-off data.[143] In this overview, Mr. Hochman

[139] Hochman Report, ¶136, FN. 104
[140] Google LLC's Fourth Supplemental Response and Objections to Plaintiffs' Interrogatories Set 1, ROG 1, p. 23-26; Ganem Depo 68:21 -73:3; Langner depo 28:23 - 32:22; Hochman Report. ¶¶ 166, 250.
[141] Hochman Report, ¶136.
[142] Hochman Report, ¶¶ 179, 248
[143] Hochman Report, ¶ 141.

concedes that only sWAA-on data could be saved to a user's Google Account for personalization.[144]

118. Mr. Hochman opines that Google can "pull the wool over its users' eyes" by storing sWAA-off data but not using it for personalization, because if Google did use it for personalization, "the user might catch on" and Google's deception would be discovered.[145] This opinion is nonsense. Taking Mr. Hochman literally would mean that Google intentionally and nefariously collects and saves, *but does not use* sWAA-off activity data for advertising because if it did use it for advertising, then the world would discover Google had secretly saved it. If this were right, then what is the activity data used for? Mr. Hochman does not explain, but the answer is plain from his report: Google saves pseudonymous data sent to it by third party app developers to provide them with analytics services. Google does not save the data to a user's Google Account when the user turns sWAA off, thereby disabling itself from leveraging the data to perform more effective, personalized advertising. Mr. Hochman does not dispute this.

119. Mr. Hochman's remaining overview of Google's data infrastructure does not tie any of its findings to the allegations concerning the saving and use of sWAA-off analytics data. Mr. Hochman's discussion in this respect amounts to a statement that Google has a complicated data infrastructure that *can* store a variety of pieces of information depending on a variety of factors. This alone does not demonstrate anything of consequence to the assignment Mr. Hochman was tasked with or to Plaintiffs' allegations.

120. Finally, Mr. Hochman addresses the test data and data from Plaintiffs' devices produced by Google. In his discussion of these data sets, Mr. Hochman details the many fields and types of information contained in analytics data stored by Google to provide analytics

[144] Hochman Report, ¶ 143 & footnote 110.
[145] Hochman Report, ¶ 144.

services to app developers. He does not, however, explain how (if at all) Google uses any of these data sets for any other purpose. For example, Mr. Hochman claims that one data field is "screenView," and this field can take a variety of values such as "RegistrationActivity" and "CartActivity," corresponding to various screens that might exist within a third-party app.[146] The "screen_view" is standard event triggered in GA4F-enabled apps.[147]

121. This information is stored by Google, even if the user had sWAA turned off, for the purpose of surfacing aggregated and anonymized information to the app developer with whom the user interacted as part of Google's provision of analytics services;[148] there is no evidence of which I am aware that Google would use the "screen_view" event for any advertising purpose when the user's sWAA is set to off, nor does Mr. Hochman explain how Google could make use of such an event, as the names of each screen are meaningful only to the app developer who names the screens, not to Google.

122. Mr. Hochman next notes that his test devices produced certain entries in baseview analytics data that contained the URL of an article the test device browsed relating to bowel movements and also contained the test device's e-mail address used to log into the app.[149] Mr. Hochman misunderstands the entries in question.

123. First, I reviewed the raw events from which Mr. Hochman excerpts the entries with the URL and e-mail address, and it is clear that these pieces of information were included by the app developer (*The Washington Post*) in a custom event created by the Washington Post. As I explain more fully in Appendix X2, apps can add virtually any extra information to a "log

---

[146] Hochman Report, ¶ 186.
[147] "[GA4] Automatically collected events," Google, available at https://support.google.com/analytics/answer/9234069?hl=en.
[148] "Measure screenviews," Google, available at https://firebase.google.com/docs/analytics/screenviews
[149] Hochman Report, ¶ 188.

event" the developer desires by setting "event_params" as they see fit. In the present case, the Washington Post app set 50 event_params including the test user's e-mail address, the URL of the article, the title of the article, the article's author, the duration of the user session, the fact the user was on wifi, something called an "identity_uid," and many other entries. These are not standard event parameters that Google includes in GA4F, and designing a custom app event that includes personally identifiable information is against Google's terms of use for GA4F and for analytics services provided by the GMA SDK (AdMob and Ad Manager).[150] That is why the vast majority of produced entries do not contain an email address. Out of 29,507 events triggered in the baseview log referenced by Mr. Hochman, 55% had no e-mail address in them, and the vast majority of the entries containing an e-mail address are from Mr. Hochman's own custom app; if we exclude all 13,344 entries from his app, then 16,009 of the remaining 16,163 entries have no e-mail address.[151] Finally, 99% of the entries had no URL in them.[152]

124. The same is true of the identifying information Mr. Hochman found in Anibal Rodriguez's and Susan Harvey's baseview data (names, e-mail addresses, phone numbers).[153] The inclusion of this information in custom events sent to Google violates Google's terms of use, and it is clear that the vast majority of events in the same data set do *not* include such data, as I have already discussed.

---

[150] "Upload data use policy," Google Analytics Help, available at https://support.google.com/analytics/answer/2838984 (last accessed May 30, 2023) ("You will not upload any data that allows Google to personally identify an individual (such as names, social security numbers, email addresses, or any similar data), or data that permanently identifies a particular device (such as a mobile phone's unique device identifier if such an identifier cannot be reset), even in hashed form. If you upload any data that allows Google to personally identify an individual, your Google Analytics account can be terminated, and you may lose your Google Analytics data."

[151] *See* GOOG-RDGZ-00071766, GOOG-RDGZ-0007167.

[152] *See* GOOG-RDGZ-00071766, GOOG-RDGZ-0007167.

[153] Hochman Report, ¶¶ 191-192.

125. Likewise, Mr. Hochman himself appears to have designed test apps that violate the GA4F terms of use by programming into them custom app events that transmit e-mail addresses. I confirmed this by reviewing Mr. Hochman's source code and analyzing his use of custom events. I also built and installed the Android apps on my Pixel 6a test phone and used a Yahoo login (johnblack.04688@yahoo.com) and logged into Mr. Hochman's app using that Yahoo login. I then confirmed that my real name and e-mail address were sent to Google by Mr. Hochman's app (in violation of Google's policy). See Appendix X1 for further details.

126. Based on my review of the stored data in question, I see no factual basis for the claim that Google designed GA4F to store any personally identifiable information when sWAA is off, such as e-mail addresses, names, phone numbers, or other similar pieces of information. To the extent such information appears in these records, it is a tiny minority of the overall events, and it was included only because an app developer, in violation of Google's terms, chose to include it.

127. Further, even where an app developer includes such information, there is no evidence that Google uses it. These are custom events, and their content is meaningless to Google, as each is custom to that app developer. At most, the e-mail addresses and other similar pieces of information sent to Google in violation of its terms remains in the siloed analytics logs kept by Google for the app developer with whom the user interacted; based on my review of the evidence in the record and the evidence cited by Mr. Hochman, I conclude that Google does not leverage, exploit, or make use of the values of these custom fields.

128. Mr. Hochman also misrepresents some other types of data found in these logs. For example, Mr. Hochman claims the logs contain detailed geographical information, but they do not. Instead, they contain an educated guess about the general geographical area where the

device was located at the time of the event. The exact way in which Google coarsens these locations is beyond the scope of this report, but Google's documents confirm that the city and/or latitude/longitude in these logs do not correspond to the user's precise location.[154] I have confirmed the same by doing testing of my own using GA4F and the test app Mr. Hochman designed. Using Mr. Hochman's app and turning on the option "granular location and device data collection" in Google Analytics, I was able to see what geographical information was logged by Google when using this app: my city, state, country and metro area were contained in the log, but there was nothing in any of the entries that would indicate my precise location.

129. Google determines the location of a user based on her IP address.[155] Many providers such as Maxmind, IP2Location, IPligence, and others, maintain a large database mapping IP addresses to estimated geographical location.[156] Google maintains a similar database and uses it to determine the approximate location of a user (note: Android on a GPS-enabled smartphone has access to very precise location information, but this is not collected by GA4F and it would be a policy violation for an app to collect GPS coordinates and send them to Google as a custom event).[157] Google does not log IP addresses in baseview, but rather stores the city,

---

[154] *See* GOOG-RDGZ-00151130, at 130 ("Geo: completed the location coarsening work across Google products.").

[155] Google LLC's Fourth Supplemental Response and Objections to Plaintiffs' Interrogatories Set 1, ROG 1, p 19.

[156] "IP Geolocation Databases: Everything You Need To Know," Geo Targetly, available at https://geotargetly.com/ip-geolocation-databases.

[157] "How does Google use location information," Google Privacy & Terms, https://policies.google.com/technologies/location-data?hl=en. ("An IP address, also called an Internet Protocol address, is a number that is assigned to your computer or device by your Internet Service Provider. IP addresses are used to make the connection between your devices and the websites and services you use. Like many other internet services, Google may use information about the general area that you're in to provide some basic services—relevant results, such as when someone does a search asking what time it is, or keeping your account safe by detecting unusual activity, such as a sign-in from a new city. Keep in mind: Devices need an IP address in order to send and receive internet traffic. IP addresses are roughly based on geography. This means that any apps, services, or websites you use, including google.com, may be able to infer and use some information about your general area from your IP address.").

state/province, and country in baseview, using the IP address to determine these values. An IP address is a relatively reliable indicator of a user's location provided Google uses a high-quality database and assuming the user is not on a VPN[158] (a big assumption given the popularity of VPNs[159]). An IP address can be used to find a user's exact position with the cooperation of the ISP, which is a technique often used by law-enforcement under warrant, but Google would not have access to this kind of confidential ISP database. Therefore Google, even if they retained IP addresses, could not determine the precise location of any given user using just an IP address.

130. Finally, Mr. Hochman implies that Google's counsel misled Plaintiffs into believing that GA4F collection logs cannot be queried by deviceID even though, later in the case, Google produced collection log entries for Mr. Hochman's four test devices.[160] Mr. Hochman fails to appreciate that Google implemented a special testing protocol that marked entries from his test devices as they entered the collection log for the purpose of producing to Plaintiffs the test data they had requested; had Google not changed its code to mark the data in this manner, it would have been logged with an encrypted deviceID, and Google would not have been able to query the collection log after the data sets were logged.[161]

b. Google Mobile Ads SDK

131. As before, my discussion of analytics data above in connection with GA4F applies equally to the aspects of GMA SDK that provide analytics services. I will discuss further here my view of Mr. Hochman's opinions as to "ads data," as he calls it, generated by GMA SDK.

---

[158] "Everything You Need to Know About IP Based Geolocation," If So, available at https://www.if-so.com/geo-targeting/.
[159] *See, e.g.*, 2023 VPN Usage Statistics, Security.org, https://www.security.org/vpn/statistics/.
[160] Hochman Report, ¶ 198.
[161] Email from Rick Strong to John Black (May 31, 2023).

132. In discussing the GMA SDK, Mr. Hochman repeats the incorrect claim that "when a user is signed into Google and has WAA or sWAA turned off, app ads data arrives at Google with both GAIA and non-GAIA identifiers."[162] That is not correct, for the reasons I discussed above. Google uses a sophisticated process relying on DSID tokens or securely managed linking tables for iOS to ensure that ads data and GAIA do not overlap in a log unless the user has provided consent, including because sWAA is turned on.[163]

133. Mr. Hochman next reiterates his understanding of the ad event data stored by Google when sWAA is off; as discussed above, it amounts to ad requests, ad impressions, and ad clicks tied to a timestamp and a device ID, usually ADID or IDFA.

134. Mr. Hochman explains that the ads logs in question contain thousands of fields, but he provides no opinion as to what the fields actually mean or under what circumstances they are filled with data, much less how Google uses them.[164] At a basic level, Mr. Hochman identifies fields that, based solely on their names, he and I agree would describe at most basic information about the device interacting with an ad and the ad in question.[165] *Id.* He notes that some fields suggest, by their name, that they can contain profiling information, but he does not explain what types of information those fields actually contain, even though Google produced some ads logs, such as conversion logs.[166] *Id.*

135. As a further note, Mr. Hochman claims but has not demonstrated that Google saves IP address in the raw with ad events information. Even if it does, I am not aware of any

[162] Hochman Report, ¶ 204.
[163] GOOG-RDGZ-00147439, at -464.
[164] Hochman Report, ¶¶ 208-212.
[165] Hochman Report, ¶ 212.
[166] Hochman Report, ¶¶ 208-212.

evidence that Google joins information together using IP address. Further, as discussed above, the IP addresses themselves are not actually logged or stored, per Google's policies.[167]

136. Next, Mr. Hochman claims that Google misled Plaintiffs relating to the relationship between ads logs and analytics logs. Mr. Hochman opines that because there are fields in the ads logs that contain the word "analytics," it suggests to him that the ads logs contain analytics data and information about whether the event in question relates to GA4F. Mr. Hochman opines that the names of these fields "reveal close ties between ads and analytics data."[168] I disagree. The names of these fields without further evidence do not reveal anything other than what they are called. Engineers call fields in databases a variety of things for a variety of reasons, many fields can be unreliable, and yet others can be used for short periods of time for specific use cases and then abandoned. Mr. Hochman does not even establish that these fields are populated in a way that would answer the question of whether Google has a bit in ads logs indicating whether an event was related to GA4F.

137. As he does in connection with analytics data, Mr. Hochman seems to characterize "record" information, such as the referrer URL of an ad or the URL of the ad itself, as the "content" the user is viewing.[169] I understand that the concept of viewing the "contents" of a communication is relevant in this case. Though I offer no legal opinion, I note here only that Mr. Hochman uses the term "content" to refer to the name, title, or URL of an article or ad, not the contents of a communication between two parties other than Google. Nor does Mr. Hochman opine anywhere in his report that Google uses such record information for any purpose other

---

[167] Mr. Hochman appears to assume IP address is included in these packets, arguing that "Google necessarily collects" it "because the IP address is part of every IP packet." Hochman Report, ¶ 130. This is not a reasonable assumption, as Google can easily ignore the IP address at logging time and therefore never "collect" or "save" the IP address.
[168] Hochman Report, ¶¶ 213-214.
[169] Hochman Report, ¶ 219.

than to report it back to app developers who collected it with their apps or advertisers who employed Google to serve their ads for bookkeeping functions.

138. To make this concrete, there is no evidence in the case that a URL such as the one in Hochman's paragraph 219–https://www.foxnews.com/entertainment/titanic-director-james-cameron-new- investigation-will-settle-jack-rose-door-debate– was ever used by Google to decipher, for example, that a particular device or user was interested in the classic debate of whether the character Jack could have survived on the floating door in the closing scenes of James Cameron's *Titanic*. These are custom events and parameters that would be meaningless to Google without additional information from the app developer. As I discuss below, the ads data Google does use for bookkeeping is far simpler and far less detailed. The rest is stored in trust for the app developer's or advertiser's use.

139. Mr. Hochman makes similar speculations throughout this section of his report. For example, he claims that Google "stores numerous ***fingerprinting*** fields" in the ads logs because he found fields that have the term "fingerprint" in them.[170] Mr. Hochman provides no evidence relating to what this field means or how it is used by Google.[171] Neither he nor I have any factual basis to conclude what the fields mean, and his speculation in this regard makes me question his reliability and credibility, especially in light of the unfounded inflammatory, adversarial language he uses throughout his report.

140. Next, Mr. Hochman discusses the pre-attribution and post-attribution conversion logs.[172] In his Appendix E, Mr. Hochman provides a high-level overview of conversion modeling and attribution. Missing from Mr. Hochman's overview are descriptions of the conversion log

---

[170] Hochman Report, ¶ 228.
[171] For example, it could relate to malware fingerprinting, not user fingerprinting. *See, e.g.*, https://securitytrails.com/blog/ja3-fingerprinting.
[172] Hochman Report, ¶ 234.

entries themselves.. Conversion log entries contain, as shown in Mr. Hochman's Appendix C, a device ID (such as ADID or IDFA), a timestamp, the app where the ad interaction occurred, the type of device and operating system of the device interacting with the ad, the rough location of the device, the conversion type, and the conversion event name (*e.g.*, "first_open"). As a result, generally speaking, the conversion logs contain only entries that indicate that a particular device engaged in a particular conversion activity on a particular app. The standard conversion events designed by Google for GA4F are: first_open, in_app_purchase, app_store_subscription_convert, app_store_subscription_renew, and purchase.[173] Thus, conversion events do not include any more detailed information about the user's activity in the app, merely a record that the user triggered a conversion event.

141. App developers can also label other events in GA4F as conversions, and they, too, would simply log that the event occurred. There are examples of this in Mr. Hochman's Appendix C, including "session_start," "view_item," and "screen_view." Again, none of these conversion events have independent meaning to Google, as they are customizable by the app developer; the conversion logs merely record that the event occurred and then, through the process of attribution Mr. Hochman describes in Appendix E, Google attempts to determine whether the same device was shown the app developer's ad so that the conversion can be counted as an advertising conversion.[174]

142. Turning to Google's [redacted] Mr. Hochman describes it as the repository of GAIA-tied and pseudonymous advertising profiles, comprising

[173] "About conversion events," Google, available at https://support.google.com/firebase/answer/6317518?hl=en#zippy=%2Cin-this-article.
[174] Knittel Report, ¶¶ 37, 92

lists of conversion events.[175] Indeed,the raw [redacted] data produced by Google in this case demonstrates what a sample conversion entry looks like in [redacted][176]:

{

column: [{

name: "com.careerkarma.chat",

cell: [{

timestamp: 1674418141687340,

Value: {

app_id: "com.careerkarma.chat",

event_name: USER_ENGAGEMENT,

source: BOW_FIREBASE,

advertiser_use_case:

[CONVERSION,REMARKETING],

platform: ANDROID,

conversion: {

event_name: "start_session"

}

}

}]

}

[175] Hochman Report, ¶ 242.
[176] Hochman Report, Appendix D.

143. As illustrated here, similar to conversion logs, each entry in [redacted] is sparse, and includes only the name of the conversion event and the fact that it happened in a particular app at a particular timestamp on a particular device.[177]

144. When a conversion event is logged by GA4F when the user has sWAA turned off, as explained by Mr. Ganem, Ms. Langner, and Google's interrogatory responses, that conversion event is not written to [redacted].[178] As a result, the conversion event cannot be used as part of any advertising profile keyed to the device or to the user's identity.[179]

145. Mr. Hochman notes that he believes that, at least in the case of Anibal Rodriguez, entries were logged from his device to [redacted] despite the fact that he had turned sWAA off on his primary Google Account, [redacted]. Thus, Mr. Hochman concludes, at least in some cases, sWAA-off data is written to [redacted]

146. Mr. Hochman is mistaken. If he were correct, then sWAA-off entries would have been in [redacted] for all the Plaintiffs as well as for Mr. Hochman's test devices. Instead, he found only these sparsely populated [redacted] entries from the ADID Plaintiff Rodriguez reported he had at the time the entries were logged. There are various technical reasons why those entries could be in [redacted], which would also explain why the entries appear in groupings at random points in time in 2021, rather than continuously throughout 2021:

---

[177] Mr. Hochman claims that "While [redacted] may contain a multitude of app information, Google only produced conversion-related data, including conversion events such as session_start, first_open, app_open, navigation, and others." Hochman Report, ¶ 246. It is unclear why Mr. Hochman assumes that [redacted] would contain more app information generated by GA4F, but I have seen no evidence that it does, and I understand from counsel that the entirety of the GA4F-generated profiles in [redacted] for the given devices was produced to Plaintiffs.

[178] Google's Second Supplemental Objections and Responses to Plaintiffs' Interrogatories, Set Six, Rog 17, at p. 15.

[179] Langner Deposition 190:16-191:5

- At the time the entries were made, the ADID could have belonged to a device that was not Mr. Rodriguez's device;
- Mr. Hochman assumed that the account logged into Mr. Rodriguez's device at the time of the [redacted] entries was [redacted], which had sWAA turned off at the time, but Mr. Rodriguez had at least twelve different accounts,[180] and there could have been others Mr. Rodriguez had at the time that he used to log into his phone.
- For example, I am informed by counsel that Mr. Rodriguez failed to disclose one account he has active on his device that had sWAA turned on during the time period of some of the [redacted] entries Mr. Hochman identifies [redacted]. (This email address differs from his primary account by one letter: the "y" in [redacted] is not present).This account could have been responsible for the [redacted] entries, but it is too late now to know, because the retention period on those logs is 530 days.
- Mr. Rodriguez indicated that he makes "spoof" emails for a variety of purposes and often will "toggle" through signed-in accounts.[181] Mr. Rodriguez may have "toggled" to a rarely-used sWAA-on Google Account, explaining why the [redacted] entries are grouped at random points in 2021.
- Mr. Rodriguez could have handed his phone to another person to use for periods of time, which would explain the use of other Google accounts associated with the conversion events recorded by [redacted].
- For example, Mr. Rodriguez could have allowed one of his children to download and install an app using their Google Account on his phone, explaining the "first_open" or

[180] Rodriguez Deposition Transcript, at 133:5-6 ("Q. Okay. So you have 12 accounts; right?" "A. Right.").
[181] Rodriguez Deposition Transcript, at 62:11-18 & 312:4-10.

"user_engagement" events recorded by [redacted] for an account that had sWAA turned on, not off.[182]

- For certain periods of time, Mr. Rodriguez could have logged out of his device entirely, preventing Google from checking his sWAA status, thereby blocking Google from being able to honor his sWAA setting; in such a state, Google could have recorded conversions to [redacted] pseudonymously.

147. Ultimately, it is impossible to know with the evidence in the record how these [redacted] entries were recorded due in part to Google's pro-privacy practice of deleting logs after a set period of time. Mr. Hochman's conclusions, however, are clearly unsupported. Whatever the explanation, it could not have happened uniformly across the proposed class, since it did not happen that way for Mr. Rodriguez himself, nor for any other Plaintiff or Mr. Hochman's test devices.

148. If I become aware of further evidence on this subject, I reserve the right to supplement this opinion.

c. Firebase Cloud Messaging

149. Firebase Cloud Messaging (FCM) is a notification platform that allows push notifications to be sent to a device configured to receive such notifications.

150. Mr. Hochman mentions FCM several times in his report, first noting its history (it was formerly called GCM), and later talking about some of its functionality with respect to

[182] Rodriguez Deposition Transcript, at 311:10-312:17 ("if [my son] has created it, I'm just going to say: Okay you created that. Now, you know what? Give me the e-mail so I can put it on my phone so I can see your-email."); 71:12-73:15 ("I might have used [the gmail account] for a game that [my son] was using…so that way I can see, you know…what he's doing on the game").

analytics.[183] In the table in Hochman's ¶ 98 he lists several FCM events that are automatically logged by GA4F. But this is seemingly the end of Mr. Hochman's opinions with respect to FCM: he offers no opinions on what data are saved on Google's servers, cites to no log analysis and offers no opinions regarding personal information being sent to Google's servers or identifiers being improperly stored. Mr. Hochman merely lists a few event types generated by FCM and moves on.

151. I have seen no evidence that event data related to FCM sends personal information or any other data that would undermine the privacy measures described for events created and sent through GA4F. Because FCM notification events are bundled along with GA4F events, they will be treated the same way when received at the backend: a separate backend server will determine if consent has been given to store the FCM event in GAIA space and if not, it will be pseudonymized as described above in this report.

3. The collection and saving of analytics, advertising, and cloud messaging data is not uniform.

152. Mr. Hochman asserts at numerous points in his report that the data collected from GA4F, GMA SDK, and GCM are "uniform." For example, he states that "Google is able to uniformly and systematically collect and save data regarding where users click, forms they fill out, what they buy, and how they interact with ads"[184] and "Google uniformly collected class members' WAA-off data and sWAA off data, including a multitude of Google identifiers that Google uses to identify particular users. These Google identifiers include class members' GAIA ID and other identifiers that Google connects with GAIA ID on its servers."[185]

---

[183] Hochman Report, ¶¶ 66, 134.
[184] Hochman Report, ¶ 3.
[185] Hochman Report, ¶ 81.

153. There is no evidence in the record to support Mr. Hochman's opinion, and he does not cite any. Further, I disagree with his opinion. Data collection through GA4F is not uniform due to the myriad ways app developers implement GA4F according to their business needs, and according to the requirement to comply with Google's terms of use. App developers who use Google Analytics for Firebase "are required by Google to disclose their use of [GA4F] to their end users [often through privacy policies] and obtain their consent, where necessary. Many such developers provide their end users with a way to opt out of analytics usage, and/or to delete data the developer has collected from that user's device and sent to Google."[186] Furthermore, as Mr. Hochman admits, "app developers have options to prevent Google from collecting data associated with their respective apps . . . For example, Google provides app developers with a setting to permanently disable all GA4F data collection or temporarily disable collection." [187] Thus Google's receipt of data from app developers through GA4F is in no way "uniform."

154. The variability in data collection is further demonstrated by Mr. Hochman and his team, who designed their own mobile applications to test GA4F data collection.[188] Mr. Hochman appears to have designed the test apps to violate GA4F terms of use by programming custom events into them that transmit email addresses. Unsurprisingly, the data transmitted by the test apps include email addresses–a clear example that the type of data collected varies greatly by the choices of the app developers. Email address collection is not a standard app event that Google includes in GA4F, and designing a custom event that includes personally identifiable information

[186] Hochman Report, ¶ 265; *See also,* Interrogatory Response, No. 18 and Interrogatory Response, No. 21, 12:19-23.
[187] Hochman Report, ¶¶ 259-260.
[188] I discuss this topic in detail in Appendix X1.

is against Google's terms of use for GA4F and for analytics services provided by GMA SDK (AdMob and Ad Manager).[189]

155. Mr. Hochman's testing also demonstrates that the vast majority of data collected by GA4F do not contain PII such as email addresses. Test devices used by Mr. Hochman and his team to collect and examine the data collected with GA4F produced certain entries in baseview analytics data that included the test device's email address used to log into the app.[190] The entry with the e-mail address, among other pieces of data, were included by *The Washington Post* app in a custom event, in violation of Google's policies. However, among all the test data collected by the devices, 16,009 of the 16,163 events triggered in those datasets had no e-mail address in them.[191] Thus by Mr. Hochman's own study, among all the apps and associated events that the test devices triggered, more than 99% did not include PII such as email addresses.

156. Conversion event logging also lacks uniformity because app developers may customize and label those events the app developer considers a conversion. Conversion logs contain entries that indicate a particular device engaged in a particular conversion activity on a

---

[189] *See*, "[GA4] Automatically collected events," Google, available at https://support.google.com/analytics/answer/9234069?hl=en&ref_topic=13367566&sjid=8747360415500982958-NA; See also, "[GA4], Custom events," Google, available at https://support.google.com/analytics/answer/12229021?hl=en&ref_topic=13367566&sjid=10112518267388711037-NA; https://firebase.google.com/policies/app-indexing#privacy_and_security (last visited May 25, 2023) (prohibiting the transmission of authentication data, among others); *See also*, "Identifying users," Google, available at https://support.google.com/publisherpolicies/answer/10436913 (Publishers must…not pass any information to Google data that Google could use or recognize as personally identifiable information"); *See also*, "Guidance for complying with the Identifying Users policy," Google, available at https://support.google.com/adsense/topic/6162392 ("In particular, please make sure that pages that show ads by Google do not contain you visitors' usernames, passwords, email addresses, or other Personally Identifiable Information [...]"); *See also*, "Google Publisher Policies: Privacy-related policies," Google, available at https://support.google.com/publisherpolicies/answer/10502938?sjid=2928812246837418863-NA#privacy ; *See also*, "AdMob policies and restrictions," Google, available at https://support.google.com/admob/answer/6128543?hl=en.

[190] Hochman Report, ¶¶ 188-189.

[191] I am excluding the 13,344 events logged by Mr. Hochman's custom app (where 98% of those contain an email address); *See* GOOG-RDGZ-00071766, GOOG-RDGZ-0007167.

particular app. The standard conversion events designed by Google for GA4F are: first_open, in_app_purchase, app_store_subscription_convert, app_store_subscription_renew, and purchase.[192] Conversion events do not include any more detailed information about the user's activity in the app, merely a record that the user triggered a conversion event. App developers can also, however, label other events in GA4F as conversion. They too would simply log that the event occurred. None of the conversion events have independent meaning to Google, as they are customizable by the app developer. Furthermore, the engagement by users varies by app and by ad. Some users may have a conversion that is purely first_open of an app, others may have lots of conversion data because they engage heavily with the app and with the ads displayed there.

157. Finally, the data sets at issue are not "uniform" because the ways that users interact with apps vary, and that will impact the collection of data about their app activity. There are users who install, but never use an app. Other users engage with apps extensively but do not have Google signals enabled. There are some that engage with an app after the first download, but stop. Some users are responsive to ads, and others who never click on or pause to view ads, so they never trigger conversion events. Some users start with android devices and switch to iOS and vice versa. The iOS 14 release, and introduction of the LAT controls impacted data transmission to app developers, which in turn impacted data transmission to Google.

C. Hochman's opinion that Google does not provide users control over Google's collection and saving of sWAA-off data is inaccurate.

158. Mr. Hochman asserts that Google "has uniformly not provided users with any control that stops Google from collecting and saving the WAA-off and sWAA-off data at issue

[192] "About conversion events," Google, available at https://support.google.com/firebase/answer/6317518?hl=en#zippy=%2Cin-this-article.

in this case" and "there is also no way to prevent Google from saving WAA and sWAA-off data once it is logged after the consent check process is complete."[193]

159. I disagree. First, it should be noted users have control over whether Google saves WAA-off and sWAA-off data to a user's account. As Mr. Hochman concedes, WAA and sWAA-off data are logged with pseudonymous identifiers, and Google makes joining pseudonymous identifiers with a user's account impossible with technological and policy barriers.[194] Thus, Google cannot make use of pseudonymous data for ads personalization for any given GAIA-identified person.[195]

160. Second, users could prevent Google from collecting WAA-off and sWAA-off data altogether by denying consent to the terms of use for app developers that collect data sent to Google through GA4F (or by declining to use those apps). Google requires app developers to disclose their use of GA4F to their end users, and to obtain their consent.[196] For example, the privacy policy for the AquaMail app discloses that:

> Google Analytics and Firebase are web and application analytics services offered by Google that track and report website traffic and application traffic and information about your device. This information is automatically uploaded to the Google servers and used to provide better services to the Users. Google uses the data collected to track and monitor the use of our Service. This data is shared with other Google services. Google may use the collected data to contextualize and personalize the ads of its own advertising

---

[193] Hochman Report, ¶¶ 249, 251.

[194] =Google LLC's Fourth Supplemental Response and Objections to Plaintiffs' Interrogatories Set 1, ROG 1, pp. 24-26; Hochman report, ¶ 250 (explaining data is logged with GAIA ID when sWAA is on, and with non-GAIA identifiers when sWAA is off).

[195] Interrogatory Response, Set 7, No. 21, at p. 13. (data generated while WAA is off is not written to [redacted] and not used for personalized advertising purposes).

[196] Interrogatory Response, Set 7, p. 6.; Hochman Report, ¶ 265; Interrogatory Response, No.18 and Interrogatory Response, No. 21, 12:19-23; Ganem Deposition, 139–411; *See also*, Interrogatory Response, Set 7, No.21, pp. 12-14.

network. For more information on the privacy practices of Google, please visit the Google Privacy Terms web page: https://policies.google.com/privacy.[197]

161. The privacy policy for the RelayforReddit app provides:

> Google Analytics for Firebase or Firebase Analytics is an analytics service provided by Google LLC. In order to understand Google's use of Data, consult Google's partner policy. Firebase Analytics may share Data with other tools provided by Firebase, such as Crash Reporting, Authentication, Remote Config or Notifications. The User may check this privacy policy to find a detailed explanation about the other tools used by the Owner. This Application uses identifiers for mobile devices and technologies similar to cookies to run the Firebase Analytics service. Users may opt-out of certain Firebase features through applicable device settings, such as the device advertising settings for mobile phones or by following the instructions in other Firebase related sections of this privacy policy, if available. Personal Data processed: Cookies; unique device identifiers for advertising (Google Advertiser ID or IDFA, for example); Usage Data.[198]

162. In many instances, I have seen app developers disclose the use of GA4F along with several other analytics providers such as Flurry and Amplitude. For example, the privacy policy for PicCollage provides:

> The information we collect from you includes the country you set your device to, the language you use on your device, the type and version of the operating system of your device, and your device model. If you make any in-app purchases, we will also collect the product IDs of the items you purchase. We collect this information from you to improve our app's overall performance and the service we provide as well as to show you ads that are personalized for you. We analyze

[197] "Privacy Policy," Aqua Mail, available at https://www.aqua-mail.com/privacy-policy/.
[198] " Privacy Policy of Relay For Reddit," Iubenda, available at https://www.iubenda.com/privacy-policy/7973777.

this information with tools provided by third party companies. These companies include Flurry, Firebase, Google, and Amplitude. You can learn more about the information they collect and analyze to ensure that PicCollage provides optimum user experience by clicking on the links above.[199]

163. The Cookie Policy for gaming app Call of Duty offers a table listing out the various cookies it uses for performance, analytics, and advertising:

a. The Properties may contain, but are not limited to, the third party Performance (or Analytics) and Advertising Cookies available through the "Cookie Settings" link in the footer of our websites and in the below list. Please follow the links below for details of the Privacy Policies and opt out choices offered by these third parties. Please also see above for further options available to manage Cookies.[200]

Online Property	**Third Party Cookies**	**Third Party Privacy Policies and Opt Out Choices**
Apps for mobile phones and tablets	Amazon Red Shift	https://aws.amazon.com/privacy/
	Appsflyer	https://www.appsflyer.com/privacy-policy/

[199] "Privacy Policy," PicCollage Company, available at https://picc.co/privacy/.
[200] "COOKIE POLICY," Activision, available at https://www.activision.com/legal/cookie-policy. (last visited May 25, 2023).

	Braze	https://www.braze.com/company/legal/privacy
	Facebook	https://www.facebook.com/policy.php
	Google Firebase	https://policies.google.com/privacy
	Helpshift	https://www.helpshift.com/legal/privacy/
	Ironsource, Supersonic	https://developers.ironsrc.com/ironsource-mobile/air/ironsource-mobile-privacy-policy/

D. Hochman's opinion that app developers have no way to prevent the collection and saving of sWAA-off data is inaccurate.

164. Mr. Hochman devotes an entire section of his report to opine that "app developers have no way to prevent Google from collecting or saving WAA-off or sWAA-off data."[201] This opinion is incorrect. For example, Google allows GA4F customers to request data deletion. This isn't just to delete all events, but also to delete specific parameters on selected events, and delete selected user properties.[202] Google also allows app developers to delete user data from the "user explorer" feature, even going so far as providing instructions for "deleting data associated with a

[201] Hochman Report., ¶¶ 258-267.
[202] "[GA4] Data-deletion requests," Google Analytics Help, available at https://support.google.com/analytics/answer/9940393.

pseudonymous ID."[203] Mr. Hochman's opinions also ignore the fact that app developers are the ones that choose what data gets shared with Google.[204] Further, app developers are required to disclose their use of GA for Firebase to their end users per the terms of service they enter into with Google, and many developers choose to provide their end users with ways to opt out of analytics usage and delete data the developer has collected from that user's device and sent to Google.[205]

165. Mr. Hochman's apparent issue is that Google does not explicitly disclose which users have turned sWAA on and which have it turned off, so that the app developer could then use this as a filter for which to delete or restrict measurement. This opinion appears to require that Google breach its own fingerprinting policies to join together and disclose pseudonymous IDs with GAIA IDs for the sole purpose that app developers can filter those categories. I am aware of no evidence that Google has done this.

E. Hochman's opinion that sWAA-off data is linked to users is inaccurate.

166. Mr. Hochman opines that "throughout the class period, Google's trove of WAA-off and sWAA-off data is linked to users."[206] I disagree. Based on my review of the evidence, I conclude that Google has made a considerable effort to separate pseudonymous data and personally identifiable data, and maintains that separation in order to ensure that WAA-off and sWAA-off data are not linked to users.

---

[203] "[GA4] User explorer," Google Analytics Help, available at https://support.google.com/analytics/answer/9283607.
[204] "Configure Analytics data collection and usage," Firebase, available at https://firebase.google.com/docs/analytics/configure-data-collection; *See also,* Interrogatory Response, Set 7, No. 18
[205] Interrogatory Response, Set 7, No. 18, 6:16-22.
[206] Hochman Report, ¶ 301.

167. Much of Mr. Hochman's opinion in this regard is focused on internal recognition at Google that joinability risks can exist and must be addressed, but he seems to misunderstand the concept of joinability risk. For example, Mr. Hochman notes that in GOOG-RDGZ-00033245, a Google witness, Xinyu Ye, lists potential joinability risks associated with a proposal then under consideration–the risks were being listed in the hypothetical sense.[207] The proposal was to store an identifier called the Firebase Instance ID in persistent storage rather than in realtime servers where it was kept in memory only.[208] In correspondence with Steven Ganem on September 18, 2020, Ye hypothesized joinability risks arising from the "ability to link app events collected by GA4F to GAIA ID."[209] The proposal to store IID to persistent server storage required approval from multiple individuals at Google, who commented on the storage design proposal for IID to ensure that joinability risks were addressed.[210] Mr. Ye was a designated "approver" for the proposal, and "[a]pproved the privacy review" for the proposal after October 16, 2020.[211] Mr. Ganem also confirmed during his deposition that IID is not stored unless a signed-in user has consented to both GAP and sWAA.[212]

168. Nowhere in Mr. Hochman's report does he identify any instance of an unauthorized joining of GAIA-tied and pseudonymous data, something that is prohibited by Google, which Mr. Hochman concedes in his discussion of fingerprinting policies.[213] Instead, he

---

[207] Hochman Report, ¶ 303. .
[208] GOOG-RDGZ-00061172.
[209] GOOG-RDGZ-00033244.
[210] GOOG-RDGZ-00061172, at 173, Comment 5 ("We should ensure no 2 humans can access both the IID <-> app instance id and IID<-> Gaiaid mapping even after running grants. This can be accomplished by making sure the humans who have access to these 2 mappings are strictly disjoint. Can you confirm that IID<-> app instance id does not exist on Firebase side?") and Comment 6:("correct no one in firebase should have iid-appinstanceid. So to ensure these two are disjoint we would use the groupbot proposal here.").
[211] GOOG-RDGZ-00061172, at 172, Comments 1-3.
[212] Ganem Deposition Transcript 214:20-215:9; 260:5-261:10
[213] Hochman Report, ¶ 228. *See* Appendix X4.

identifies joinability risks as he sees them. To be clear, I understand joinability risk to be a version of insider risk: in essence, the concern is that a bad or negligent actor within Google would perform an unauthorized join, violating Google's internal policies.[214] Google not only forbids unauthorized joins and monitors its systems for unauthorized joins, but it devotes significant resources to identifying and mitigating joinability risk so that no employee of Google can violate the policies even if they wanted to.[215]

169. Mr. Hochman claims that, because Google uses similar structures in analytics logs and GAIA logs, that necessarily means that "the timestamps, identifiers, and data stored in both types of logs make GAIA and non-GAIA data and ID joining straightforward."[216] He cites no authority or evidence for this proposition. Nor does he provide any evidence that such joining has ever happened. Further, Mr. Hochman ignores that Google takes significant steps to mitigate joinability risk by scrubbing and blurring timestamps, encrypting identifiers using different encryption keys in different logs, and ensuring data fields in GAIA-tied logs do not overlap with fields in non-GAIA logs, or are encrypted differently so that they cannot be joined. And he repeatedly argues that, because fields appear in multiple log sources with the same name, such as app_instance_id or IPv4 address, that means joinability risks persist at Google.[217]I disagree. Mr. Hochman notably does not identify the *same* app_instance_id in GAIA-tied and non-GAIA-tied logs, and that is because they are encrypted differently in different logs.[218] Likewise, Google

[214] Interrogatory Response, Set 1, No. 1
[215] ROG 1, p. 23-26 Ganem Deposition Transcript; 260:14-19
[216] Hochman Report, ¶ 202.
[217] Hochman Report, ¶ 248.
[218] Ganem Deposition Exhibit 202, at -27638; GOOG-RDGZ-00184459 at-4462; GOOG-RDGZ-00061172

obscures IP addresses; while they may still look like IP addresses, they will not match up to the user's true IP address or to each other across logs. The same is also true of timestamps.[219]

170. More specifically, Mr. Hochman states that "several events contain both GAIA ID and encrypted app instance_id.[220]" He then refers to his Appendix G for support; there he refers to a "hashed app_instance_id" in tmpapp_measurement[221], the actual app_instance_id of apps installed on his test devices[222], and an "encrypted app_instance_id."[223] Mr. Hochman never claims that these different instances of app_instance_id can be matched up precisely because they cannot be: the original value is different from the hashed value, which are both different from the encrypted value. Take for example the app "com.matteljv[redacted]" which was installed in Mr. Hochman's test device "Android 1." The app_instance_id given in his Appendix B.3, "2023-02-23 App and Instance IDs" tab, for this app is cc35233d8867471f9636bbca5eb6a6d5. This is the actual app_instance_id. The "hashed app_instance_id" found in his Appendix H.2, "198334 Pseudo Analysis" tab, column AE, is "[973022505764608054]" for the same app. And in the "encrypted app_instance_id" given in Appendix F, "Adevents Analysis" tab, column T is a 101-character base64-encoded ciphertext with the value "CkUKEAiAiJSeBhDs0dSZ1KuqzFUSMQA8MScJVyuXkeycAWV3KLQcwzJFTwCtJUAEIWuS0JjFqGJd1X+DAb271IGiZLC9ivcQAA==" again for the same app. In this example, the original true value for app_instance_id is not reflected in any Google log, and the two instances Mr. Hochman points to showing transformed values of app_instance_id are incomparable because they have been transformed in two different ways.

---

[219] GOOG-RDGZ-00207669.
[220] Hochman Report, ¶ 248.
[221] Hochman Appendix G, ¶ 34, Appendices H.1, H.2.
[222] Hochman Appendix G, ¶ 75, Appendix B.3.
[223] Hochman Appendix G, ¶ 95, Appendix F.

171. With respect to the transformed values stored in Google's logs, Mr. Hochman states that "Google has the hash function" and therefore can use the submitted app_instance_id to locate records[224]. But this does not explain how Google could use a hashed app_instance_id to identify a user (or even recover the original app_instance_id) and therefore does not explain how storing a hashed app_instance_id could in any way represent a breach of user privacy. With respect to encrypted app_instance_id, Mr. Hochman states that "Google can decrypt these values" and thereby identify users.[225] However, Mr. Hochman fails to explain how someone at Google would obtain the necessary decryption keys in order to reveal the original app_instance_id; as I have explained previously in this report, cryptographic keys are tightly controlled at Google.

172. Next, Mr. Hochman claims that sWAA-off data is "linked to users" because Google has the ability to check users' privacy control settings, and therefore must be *able to* link a user's identity to their pseudonymous identifiers.[226] This is not a logical conclusion. Google checks for consent for data sent to Google from Android and iOS devices via GA4F and GMA SDK in order to honor user privacy settings. That does not also mean that it necessarily joins sWAA-off data to a user's identity; indeed, the opposite is true: when sWAA is off, Google takes multiple technical steps to ensure the data cannot be joined to the user's identity, as I have discussed elsewhere in this report.

173. Next, Mr. Hochman claims that because conversion attribution is performed using, among other identifiers, DSID, this necessarily means that "Google in effect associates WAA-off and sWAA-off data with GAIA." [227] This is incorrect; as I have described elsewhere in

---

[224] Hochman Appendix G, ¶ 47.
[225] Hochman Appendix G, ¶ 95.
[226] Hochman Report, ¶¶ 305-307.
[227] Hochman Report, ¶ 310.

this report, DSID is not GAIA, and it cannot be used to decipher a user's identity unless it is sent to the user identification server, which decrypts DSID and returns information about the user's privacy control settings.[228] Mr. Hochman provides no evidence for the claim that Google associates sWAA-off ads data with a user's GAIA, or their identity, other than this unsupported assertion.

174. Mr. Hochman lists and describes various ID linking efforts by Google, including [redacted], and [redacted]. I am not aware of any evidence that any of these ID linking efforts involve associating pseudonymous identifiers with a user's identity, nor does Mr. Hochman claim otherwise.[229]

175. Mr. Hochman also notes that app developers can create their own third-party user IDs, which would be unique to a particular user across devices.[230] This is publicly documented functionality for GA4F. As Google explains, "The User-ID feature lets you associate your own identifiers with individual users so you can connect their behavior across different sessions and on various devices and platforms."[231] And, Google warns app developers: "You're responsible for ensuring that your use of the user ID is in accordance with the Google Analytics Terms of Service. This includes avoiding the use of impermissible personally identifiable information, and providing appropriate notice of your use of identifiers in your Privacy Policy. Your user ID must not contain information that a third party could use to determine a user's identity."[232] Mr. Hochman does not acknowledge this limitation of the user ID feature, nor does he provide any

---

[228] *See infra* Paras. 34, & B.1.a.i., 2.a.i.

[229] Hochman Report, ¶¶ 318 - 324.
[230] Hochman Report, ¶ 325.
[231] "[GA4] Measure activity across platforms with User-ID", available at https://support.google.com/analytics/answer/9213390?sjid=8267222974802622658-NA.
[232] "[GA4] Measure activity across platforms with User-ID", available at https://support.google.com/analytics/answer/9213390?sjid=8267222974802622658-NA.

evidence that Google uses third party user IDs for any purpose at all other than to provide analytics services to app developers. I am aware of no evidence that suggests third party user IDs mean anything to Google at all; indeed, each app developer would have their own way of generating these user IDs, and there would be no standard way for Google to decipher them.

176. I do note, however, that Mr. Hochman appears to have violated the Google Analytics Terms of Service in the design of his test apps, which send both the user's real name and email address (obtained from Yahoo) to Google's analytics server.[233]

177. Mr. Hochman next argues that there is joinability risk because he was able to obtain both his own GAIA and his own ADID using Google Takeout and documents produced by Google in this case.[234] Mr. Hochman ignores, however, that without the cooperation of the user himself, Google would not be able to associate the ADID and GAIA, doing so would violate Google policies, and there are technical barriers in place to prevent it from happening, including encryption, as I have discussed above. That Mr. Hochman can unmask himself does not mean that Google can or does. Mr. Hochman's report does not identify any instance of an unauthorized join or unmasking performed by Google, nor does he cite to any evidence that suggests this has ever happened. As I have discussed, at most, Mr. Hochman argues there is a theoretical possibility that Google could, with malicious intent and added effort, unmask an individual's pseudonymous analytics or ads data. Maybe so, but that risk is theoretical; I am not aware of any instance of it happening, and it does not represent Google's technology as it is designed and as it has been employed throughout the class period. To the contrary, the evidence in this case

[233] *See* Appendix X1 - Notes on Building, Running, Modifying and Testing Plaintiff's "WAA Toggle" Custom App

[234] Hochman Report, ¶ 330.

demonstrates that Google has invested tremendous resources into preventing just such an "unmasking" from occurring.

178. Mr. Hochman's concerns about the theoretical possibility of an unmasking is evident again in his discussion of Google's encryption practices. He posits that "Merely decrypting these IDs would join them to a user's GAIA ID."[235] Leaving aside that decrypting the IDs alone would not join them to anything, more importantly, Mr. Hochman's opinion here is again speculative; he does not cite to any evidence indicating that such a join has occurred or that Google's system is designed to perform such joins. Additionally, Mr. Hoffman says "*merely* decrypting" as if decryption is a simple and straightforward task easily performed by anyone at Google; he fails to mention that decryption of ciphertexts produced by modern encryption systems is intractable even for experts unless one possesses the decryption key, and (as I have noted previously) such keys are tightly controlled by Google.

179. Mr. Hochman offers an opinion that "although Google refers to advertising IDs as 'pseudonymous' IDs, these IDs uniquely identify a user's device [...].[236]" Mr. Hochman appears to believe that an ID tied to a specific device violates Google's claim that such IDs are pseudonymous, but this is clearly incorrect; in fact, replacing personally identifiable information with a random number is exactly what it means to use a pseudonymous ID.

180. Mr. Hochman goes on to state that the Electronic Frontier Foundation (EFF) supports his opinion, and he includes a block quote from an EFF article that enumerates the dangers of using pseudonymous identifiers. The quote (and the EFF article from which it is excerpted) explains that identifiers like the ADID can tie a given user's activities together from

[235] Hochman Report, ¶ 331.
[236] Hochman Report, ¶ 311.

different sources. The author reasons, therefore, that there is a risk to user privacy in the use of such IDs.

181. It is true that there are risks that a well-resourced and ethically questionable organization could piece together various pieces of data and abuse it to learn about someone based on ADID and other similar pseudonymous IDs. The EFF article links to a Motherboard article[237] that explains this further: there are certain "shady data brokers" who will sell this kind of information after "unmasking" targeted users. But of course, Google is not one of those, and there is no evidence of which I am aware that Google sells the data to "shady data brokers," nor does Mr. Hochman claim that it does. The risks associated with unscrupulous entities using a pseudonymous identifier simply do not relate to Google; that such a tool can be misused does not mean Google has, will, or has intended to do so.

182. Finally, although Mr. Hochman opines (and I agree) that pseudonymous identifiers carry some risk, he does not explain how a risk to privacy constitutes an *invasion* of privacy. In other words, Mr. Hochman's opinions with respect to pseudonymous identifiers fail to identify any actual harm, only the risk of one.

183. I note here that Mr. Schneier also opines regarding joinability risk, parroting much of what Mr. Hochman says and the same evidence he cites, in paragraphs 216-221 of his report. My opinions here as to joinability risk apply equally to this section of Mr. Schneier.

F. Hochman's opinion that Google monetizes sWAA-off data is inaccurate.

184. Mr. Hochman opines that Google monetizes the sWAA-off data he discusses in his report by "serving advertisements, tracking and modeling conversions, and improving

[237] "Inside the Industry That Unmasks People at Scale", Vice, available at https://www.vice.com/en/article/epnmvz/industry-unmasks-at-scale-maid-to-pii

Google products, processes, and services."[238] I disagree. Mr. Hochman fundamentally misunderstands how Google uses the sWAA-off data in question.

185. The principal sWAA-off data Mr. Hochman accuses Google of monetizing is ads-related data (as opposed to analytics data logged by GA4F or the equivalent analytics service in GMA SDK). This appears to be because Mr. Hochman cannot claim that any sWAA-off analytics data is used directly to profit, since, as Mr. Hochman concedes, Google does not personalize advertising with sWAA-off data, contrary to the central allegation of Plaintiffs' complaint.

1. Ad Record Data

186. The ads-related data Mr. Hochman focuses on falls into two categories. First, Mr. Hochman discusses what I will call "ad record data." These are data components indicating an ad request has been made, or an ad has been served, to a device. Mr. Hochman states, for example, that ad requests are sent to Google's server regardless of the user's sWAA status.[239] In referring to this category of data, Mr. Hochman opines that "but for Google's collection of WAA-off or sWAA-off data, Google would not be able to serve advertisements to those users and then charge the advertisers because Google would lack the necessary data records to back up their advertising charges."[240]If I understand Mr. Hochman correctly, he argues that when a user has sWAA turned off, apps that use the GMA SDK should not be permitted to serve ads to the user at all, because doing so would require sending an ad request to Google (even though the same app could use any other advertiser network to do the same thing). In other words, Mr. Hochman argues that the WAA and sWAA controls were meant to serve as total ad blockers for apps that use Google's

[238] Hochman Report, ¶ 268.
[239] Hochman Report, ¶ 272.
[240] Hochman Report, ¶271.

advertising network. And, he therefore concludes, since the sWAA control would block advertising, by definition the "service record" information used to request and serve an ad is being monetized by Google.

187. This logic is circular and unhelpful, and as far as I can tell, Mr. Hochman has applied no expertise to performing it. The opinion that because all data generated by an app is "app activity" data, and so the sWAA button must block all data from an app when sWAA is off defies the purposes of the WAA and sWAA buttons as described by Google, defies common sense, and ignores the multitude of other controls available to the user on the same page and through other tools to fine-tune how Google collects and uses data. For example, a user could choose to have Ads Personalization turned on but sWAA turned off (meaning sWAA off data should not inform the personalization of ads, but ads should be personalized with data collected when sWAA was on); indeed, this is precisely what named Plaintiff Sal Cataldo testified was his intention when he turned GAP on and sWAA off.[241] Yet, per Mr. Hochman, his choice was incorrect, because when sWAA is off, *no* ad serving should be possible, even when the user has indicated they *want* ads, and they *want* those ads to be personalized. As I have discussed elsewhere in my report, the reason Mr. Hochman's opinion breaks down here is that an ad request is not, in any reasonable technical sense, "app activity" data, but rather basic ad record data used to facilitate the basic functioning of the app, no different than bookkeeping to keep track of ads aired on television or published in magazines.

2. "Targeting" as Distinct from "Personalization"

188. Next, Mr. Hochman argues that, even though Google does not personalize advertising using sWAA-off data, it does "target" advertising using sWAA-off ad record data. In

[241] Cataldo Depo. at 152:18-153:18.

this, he commits another logical fallacy. Mr. Hochman notes that Google's witnesses and documents indicate that Google does not use sWAA-off data for personalization, but generally speaking, advertisers can target their ads to specific audiences based on location data and other similar types of data; and, he says: "I have not found any information indicating that Google is unable to use these types of WAA-off and sWAA-off data to serve targeted advertisements."[242] Thus, he concludes, it must be that Google is targeting advertising using sWAA-off data. In making this conclusion, he appears to be saying that without evidence of a negative, he concludes the positive must be true.

189. This is, of course, not expert opinion; it is a classic logical fallacy that is unsupported in the evidence. Rather than engage in Mr. Hochman's word game, I opine here on the technical information I understand from the same evidence Mr. Hochman reviewed. There is no evidence that Google uses sWAA-off data to personalize advertising, and there is substantial evidence that by policy, design, and practice, it takes steps to ensure it does not do so; Mr. Hochman acknowledges some of this same evidence in this section of his report. [243]As for ad "targeting," Mr. Hochman seems to be conflating a consumer-facing term (where advertisers are the consumer) and a technical term, arguing that "Google in this case seems to be making a distinction between 'personalization' and targeting."[244] I have not seen anywhere where Google has made this distinction. Mr. Hochman screenshots a list of targeting options for advertisers, but does not indicate which options will leverage sWAA-off data and which cannot. Nowhere else in his report does he provide any evidence that Google uses sWAA-off "app activity" data to target advertising. Google does refer to contextual non-personalized advertising, and none of this is

[242] Hochman Report, ¶ 277.
[243] Hochman Report, ¶ 276.
[244] Hochman Report, ¶ 277.

implicated by Plaintiffs' allegations.[245] For example, advertisers can ask Google to target ads to a particular geography, just as an advertiser on television can, or to a particular app or article, just as a magazine advertiser can. This is no more personalized as those legacy forms of advertising are. None of it uses historical "app activity" data to decide which ad to serve to a user.

190. Mr. Hochman does surmise that Google could use a user's IP address to infer location, and target advertising based on that; but, of course, an IP address is not "app activity" data, and so it is not clear why that would be relevant here. Nor would it be relevant if Google advertises based on a user's device and operating system, since neither of those are "app activity" data, either.

191. Mr. Hochman also takes pieces of Google's interrogatory responses out of context to suggest that Google itself admitted that it targets advertising using sWAA-off data, even if it does not personalize.[246] I have reviewed these interrogatory responses, and that is not what they say. In its response to Interrogatory No. 1, Google explained that "Google can also use pseudonymous event data from GA for Firebase logs to target advertising to users, all without personally identifying the user. Users can opt out of such ad targeting on their device by opting out of ad tracking on their Android or iOS device.."[247] This is a true statement, but does not indicate what happens when sWAA is turned off, and how targeting is limited under those

---

[245] *See, e.g.*, "Personalized and non-personalized ads", Google AdMod Help, available at https://support.google.com/admob/answer/7676680?hl=en (distinguishing between personalized and non-personalized advertising; explaining non-personalized advertising means users "are targeted using contextual information, including coarse (such as city-level) geo-targeting based on current location, and content on the current site or app or current query terms" rather than "based on previously collected or historical data to determine or influence ad selection, including a user's previous search queries, activity, visits to sites or apps, demographic information, or location. Specifically, this would include, for example: demographic targeting, interest category targeting, remarketing, targeting Customer Match lists, and targeting audience lists uploaded in DoubleClick Bid Manager or Campaign Manager 360.").

[246] Hochman Report, ¶ 276.

[247] Google's Fourth Supplemental Response to Interrogatory No. 1, p. 28, 29.

circumstances. Other sections of this and other interrogatory responses as well as documents and deposition testimony, address those questions, and explain that Google does not personalize advertising using sWAA-off data, as I have discussed throughout this report. In its response to Interrogatory No. 15, Mr. Hochman notes, Google wrote that "it uses data sent to it via Google Analytics for Firebase for each of the uses described in its Privacy Policy and Google Analytics for Firebase Terms of Service, according to the settings and consents provided by both end users and Firebase customers. This includes pseudonymous conversion tracking and ad targeting for anonymized ad profiles." But Mr. Hochman ignores the supplemental response Google provided that further explains this concept: "When a user is signed in and has sWAA off, app activity data sent to Google via GA4F while sWAA is off cannot be used for personalization. If a user is signed out on a device and also happens to have one or more Google accounts that have sWAA turned off at the time of app activity in a GA4F-enabled app on that device, that app activity data could become part of an anonymized ad profile for ads personalization." From my review of Plaintiffs' interrogatory, it appears that Plaintiffs' definition of "WAA OFF data" for purposes of that interrogatory caused confusion as to whether signed-out data for a person who has a Google account with WAA off, but for whom Google cannot determine WAA is off, constituted "WAA OFF data" within the meaning of Plaintiffs' question. In any case, the evidence I have reviewed is consistent with the further explanation in Google's supplemental response.

192. Finally, Mr. Hochman notes that there are other privacy controls at play here. That is, indeed, true. Users can have GAP turned on, indicating a desire to receive personalized advertising. They can also have NAC turned on, indicating a desire to connect their activity data on third party apps to their activity on first party apps and websites.[248]Conversion Measurement

[248] Hochman Report, ¶ 278.

193. The second bucket of ads-related data Mr. Hochman opines Google monetizes is conversion measurement data. As distinct from what I call "ad record" data, conversion measurement data connects a piece of analytics data to ad record data to form an inference about whether an action in a third party app from a particular device or user came from the same device or user that interacted with an ad from the app developer earlier in time. From my review of the evidence and the claims Mr. Hochman makes in his report, I conclude that Mr. Hochman's opinion that Google monetizes conversion measurement data is not factually supported, and that there is no evidence to conclude that Google uses conversion measurement data in the way Mr. Hochman suggests.

194. I understand from Dr.. Knittel's report that conversion measurement involves adtech systems in use, the type of app, the user's privacy settings, and other factors.[249]

195. Mr. Hochman agrees, stating that "The ability to capture conversion events, as well as the ability to attribute a conversion event to a prior ad event, allows Google to demonstrate the effectiveness of its advertising platforms to the advertisers, which in turn, increases advertiser spend on Google advertising platforms."[250] Mr. Hochman also describes the conversion measurement process in general detail in his Appendix E. According to Mr. Hochman, "But for Google's collection and saving of WAA-off or sWAA-off data, Google would not be able to attribute conversions to events (like ad clicks) that occur when WAA or sWAA is off."[251]

196. Mr. Hochman next concludes that Google must therefore be profiting from conversion measurement data, but his opinion on this is severely lacking. He first claims that

[249] Knittel Report, ¶¶ 31-35, 74
[250] Hochman Report, ¶ 280.
[251] Hochman Report, ¶ 280.

Belinda Langner explained how "Google ultimately benefits from its ability to track conversions" by quoting a section of Ms. Langner's deposition where she is *not* discussing how Google benefits from its ability to track conversions, but instead is discussing how *advertisers* benefit from conversion measurement.[252] Just a page later in the transcript. Ms. Langner was directly asked how Google benefits from conversion measurement, even when the user has sWAA off, and she answered that Google has never studied it, but that generally speaking Google is providing a service for advertisers to be able to measure the performance of their ad campaigns but does not directly profit from conversion measurement:

> Q. With regard to these -- these revenue streams, does Google make any money from ad conversions, tracking ad conversions?
>
> A. So Google specifically and app campaign specifically's goal is to drive -- to drive users for these advertisers that are more likely to perform these specific actions. It is -- and we do conversion measurement as a way to show the value that the Google app campaigns have brought to a specific advertiser.
>
> Q. What about conversions for when sWAA is off, does Google make any money off of that?
>
> A: I think we've sort of talked about the sort of app measurement concept already, right? So for the purposes of advertising, Google wants to demonstrate the value of our app campaigns, app conversion measurement allows us to demonstrate the value that Google Ads drives for that specific advertiser.

[252] *See* Hochman Report, ¶ 288, quoting Langner Tr. at 213-214.

> Q. So then what's the purpose of measuring a sWAA-off traffic for the purposes of conversions for these revenue streams?
>
> A: When advertisers use app campaigns, they want to know how well their app campaigns are doing, just like they would want to know how well their campaigns on other ad networks are doing. So across the board, advertisers do use measurement platforms such as GA4F or other ad app attribution partners to measure the performance of their campaigns, be it the Google app ads campaigns or other campaigns. And the whole purpose of that, right, is so that advertisers understand how they should distribute their budget between the various different ad networks that they are advertising with.[253]

197. Mr. Hochman takes from this testimony that "Google's trillion-dollar advertising engine ***relies on*** ad performance measurements that report to advertisers how effective their ads have been and prove that Google's ads meet industry standards for traffic quality."[254] This reliance, he posits, means that Google monetizes the sWAA-off conversion measurement data. But one does not follow from the other. The same chunk of testimony explains that advertisers need not use Google to measure conversions at all; they can use "other ad app attribution partners to measure the performance of their campaigns."[255]

198. Google explains the technical details of how to measure conversions using an app attribution partner on its public documentation pages.[256] At a technical level, this process is

[253] Langner Deposition Transcript, at 215:2-216:22.
[254] Hochman Report, ¶ 290.
[255] Langner Deposition Transcript, at 216:14-16
[256] *See, e.g.*, "Set up conversions from Firebase or App Attribution Partners for App campaigns for engagement," Google Ads Help, available at https://support.google.com/google-ads/answer/9260620.

simple. Rather than using GA4F or GMA SDK to measure conversions, an advertiser would use another analytics and conversion measurement provider's SDK in their app. There are many, such as Kochava and AppsFlyer. Like GA4F and GMA SDK, the SDKs from Kochava and AppsFlyer measure activity in the app, including custom and standard conversion events.[257] These apps can then export conversion data directly to Google's ads product, which helps app developers determine how well their advertising campaigns worked on Google's display network.[258] The third party SDKs also permit app developers to send the same conversion data to other ad networks, including Facebook, Apple, and Twitter:

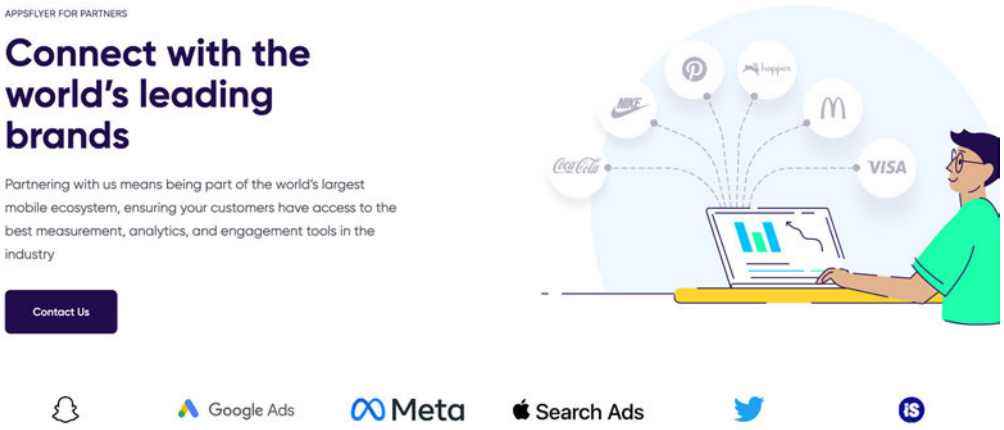


Figure 1. AppsFlyer's partners page[259]

199. In this way, an app developer can use a single SDK to measure conversion activity, but advertise their app on all of the major ad networks, not just Google's ad network.

[257] *See* https://support.kochava.com/sdk-integration/android-sdk-integration/android-using-the-sdk/; https://support.appsflyer.com/hc/en-us/sections/6551285343761-In-app-events.
[258] *See, e.g.*, "Google Ads", Kochava Support, available at https://support.kochava.com/campaign-management/google-ads/
[259] "Connect with the world's leading brands", AppsFlyer, available at https://www.appsflyer.com/solutions/partners/.

200. Likewise, app developers can use GA4F to measure conversions generated by ads placed on the other ad networks, and then join that information with information from the ad networks to measure advertising campaign performance, though doing so requires additional work compared to using AppsFlyer or Kochava, because GA4F does not natively support integrating with ads from other ad networks.

201. Perhaps for this reason, third party analytics SDKs are very popular. Many apps use multiple analytics SDKs, and disclose that they do in their privacy policies. *See* Appendix X5. In this case, there is evidence that until recently, GA4F was rarely used to measure conversions, even for ads run on Google's ad network, but through more recent promotion efforts called [redacted], which are described by Mr. Hochman in his Appendix E, the percentage of ad campaigns run that bid on Google Analytics conversions has risen to [redacted], leaving [redacted] to be bid on conversion data from a different source than Google Analytics.[260]

202. The method of conversion attribution of the third party conversion measurement providers is functionally identical to the methods used by Google, except that because end users don't have pre-existing relationships with those providers, those providers cannot also respect the users' privacy settings to, for example, prevent personalized advertising. Below, for example, is a table from AppsFlyer describing the various ways in which an app with the AppsFlyer SDK can generate data that AppsFlyer will use to attribute conversions to ad events:

[260] Google's Supplemental Responses to Interrogatory Set 6, Rog 17, at p. 15-16. See also Hochman App'x E.

Method	Uses an ID	Technique	Attributed by	Android (1)	iOS	Window Universal Platform	CTV and gaming platform (3)
Referrer	Yes	Deterministic	AppsFlyer	Yes (2)	No	Yes	No
Device ID matching	Yes	Deterministic	AppsFlyer	Yes	Yes	Yes	Yes
Probabilistic modeling	No	Probabilistic	AppsFlyer	Yes	Yes	No	Yes
Aggregated Advanced Privacy (AAP)	No	Aggregate	AppsFlyer	No	Yes	No	No
Preload	No	Deterministic	AppsFlyer	Yes	No	Yes	No
SKAdNetwork (SKAN)	No	Deterministic	Apple	No	Yes	No	No
Apple Search Ads	Yes	Deterministic	Apple	No	Yes	No	No
Deep link	No	Deterministic	AppsFlyer	Yes	Yes	Yes	No

(1) Google Play and third-party stores

(2) Supported by some third-party stores

(3) See full list of CTV and gaming platforms

Figure 2. Example of data that will use to attribute conversions to ad events[261]

203. The work involved in integrating an SDK is not particularly significant. SDK providers endeavor to make their SDKs work "out of the box" for as many customers as possible. And products like AppsFlyer's and Kochava's are free to use, though premium offerings are available from each of them (as well as through Google with GA360) through premium pricing. I discuss third party analytics providers in more detail in my Appendix X3.

204. At a technical level, the conversion measurement of GA4F as opposed to third party providers is relatively fungible; the purpose of the endeavor is to measure conversions accurately, and depending on features and a particular app developer's needs at a moment in

[261] https://support.appsflyer.com/hc/en-us/articles/207447053-AppsFlyer-attribution-model.

time, one or the other offering may be more ideal. There are hundreds of third party providers competing for mobile app developers in this space, and more starting up every year.

205. At bottom, these measurement efforts are valuable to advertisers, with the goal being accurate measurement. But when advertisers run ads on Google's ad display network, they are not paying per conversion, nor does the measurement of conversions translate in literal terms to payment. Instead, app developers engage in autobidding, which provides Google with a budget for an ad campaign and desired target number of conversions. Advertisers can choose how to measure the conversions, and which SDK will measure them. But the payment is for the placing of ads in Google's display network.[262] Sometimes, advertisers will prioritize app installs, which by itself is not "app activity" data so much as information concerning whether the device installed the app or not. Other times, advertisers can focus on in-app events, and will program their analytics SDK (whether GA4F or a third party SDK) to record a conversion when a particular in-app interaction occurs.

206. Conversion measurement is therefore not monetized by Google. At most, the relevant question would be what app developers who spend money on Google Ads would do if GA4F did not provide conversion measurement information for sWAA-off users on Android (on iOS, because of changes iOS 14, Google now cannot confirm a user's privacy settings, as discussed elsewhere in this report). Because of the plentiful variety of analytics providers in the market and the evidence suggesting app developers have long used conversion measurement services other than Googles' services in GA4F and the equivalent infrastructure in GMA SDK, it

[262] *See generally*, "The ultimate guide to Google App Campaigns", App Radar, available at https://appradar.com/academy/google-app-campaign; see "About bidding in App campaigns", Google Ads Help, available at https://support.google.com/google-ads/answer/7100895?hl=en; "About automated bidding", Google Ads Help, available at https://support.google.com/google-ads/answer/2979071?sjid=14720596150785634323-NA.

is my opinion that an advertiser's first reaction in this situation would be to rely on other analytics SDKs already installed in the app, or to begin exploring other analytics SDK options.[263] In my opinion, the big players in this market, like Kochava and AppsFlyer, would provide substantially identical conversion measurement accuracy to app developers, so the cost to developers in this situation would be the cost of switching the configuration of which SDK is used to measure conversions or the cost of integrating a new SDK into the app.

207. Based on my experience, in my opinion, integrating AppsFlyer was very easy, and the average app developer with a non-trivial advertising budget would not hesitate to integrate this new SDK if GA4F stopped measuring sWAA-off conversions. I cannot think of any reason why an app developer would, instead of using a third party conversion measurement service, choose instead to cease advertising with Google, or even lower their advertising budgets with Google, due to GA4F measuring only sWAA-on and logged-out conversions.

208. A version of this experiment has, in fact, already played out. After iOS 14 released, the ability to track conversions using GA4F and many other analytics SDKs was impaired by Apple's policies surrounding device IDs. Since iOS 14, apps must ask a user for permission to obtain the user's IDFA, which can subsequently be used to measure conversions by analytics providers and advertisers. If the user declines permission, the app developer must find another way to measure conversions. Apple provided one such alternative, though there are others. That alternative is SKAdNetwork,[264] which, as AppsFlyer explains, "helps ad networks and advertisers measure their ad activity (such as impressions, clicks, and app installs) on an aggregated level."[265] SKAdNetwork has actually been around since long before iOS 14; it was

---

[263] Knittel ¶¶ 97, 123-24

[264] "SKAdNetwork", Apple, available at https://developer.apple.com/documentation/storekit/skadnetwork/.

[265] "SKAdNetwork(SKAN)", AppsFlyer, available at https://www.appsflyer.com/glossary/skadnetwork/.

introduced in 2018, and it supplies one alternative to the method of conversion measurement employed by AppsFlyer, GA4F, GMA SDK, and a variety of other analytics providers by simply counting conversions within Apple and reporting the number of conversions to the app developer without reporting any user's device ID.[266] Although SKAdNetwork does not provide the typical way of measuring conversions, in AppsFlyer's view: "measurability has been mostly retained with improvements driven by better models, increased usage of predictive analytics, acquired expertise in SKAN, and innovation across the ecosystem."[267] Thus, although changes in iOS 14 initially suggested that conversion measurement impairment would impact the advertising industry, at least as to conversion measurement the technical tools available to measure conversions while shielding pseudonymous identifiers entirely have only continued to improve, leaving advertisers/app developers little reason to advertise less, insofar as their decision-making is driven by the accuracy of conversion measurement.[268]

209. It is also notable that a substantial portion of conversions "recorded" by Google during the class period were not based on any sWAA-off data at all, though exactly what proportion is impossible to determine. As Mr. Hochman and Mr. Knittel explain, conversion modeling has become very popular among advertisers, analytics providers, and ad networks. Because of this, it is impossible to know if recorded conversions relate directly to an ad event or conversion event recorded by GA4F or GMA SDK; it is just as possible that the conversion was modeled using information acquired by Google from sWAA-on users.[269]

---

[266] "SKAdNetwork(SKAN)", AppsFlyer, available at https://www.appsflyer.com/glossary/skadnetwork/.
[267] "SKAdNetwork(SKAN)", AppsFlyer, available at https://www.appsflyer.com/glossary/skadnetwork/.
[268] Other tools have cropped up in the wake of iOS 14, including deep linking, private relays, and others. The specifics of these tools is less important here than to note that, one way or another, app developers can measure conversions in their own apps, even if they are not permitted to rely on Google to do it.
[269] Knittel ¶¶ 29-38.

3. Marginal Costs of Measuring sWAA-off Conversions and Analytics Activity

210. Mr. Hochman opines in this section of his report as follows: "it also is my opinion that Google's collection and saving of WAA-off and sWAA-off Data does not result in any material incremental costs to Google's business. WAA-off and sWAA-off Data constitutes a relatively small portion of traffic compared to WAA- on and sWAA-on Data. Therefore, Google's collection and saving of WAA-off and sWAA-off (or Google's lack of doing so) has no material impact on Google's planning and budgeting for infrastructure, including physical space, data warehouse capacity, personnel, and marketing."[270]

This opinion contains no citations to authority or evidence. I am unclear on how exactly Mr. Hochman developed this opinion, as I am aware of no evidence he relied upon or that I have been provided by counsel that measures the marginal costs of measuring conversions or ads-related data, or analytics data, of sWAA-off users. I am aware, however, that storage of sWAA-off data is exceedingly expensive, as is all storage.[271] In this case, Google estimated in a sworn declaration that just storing baseview data costs Google $3 million for two years' worth of storage and $6 million for three years. This does not include, for example, the cost of running those data centers, the cost of running the analytics program, and the cost in human resources, facilities, etc. in servicing analytics customers.

4. Improving Google Products, Processes and Services

211. I understand, as Mr. Hochman recites, that Google's interrogatory responses state that "GA for Firebase allows sharing Analytics data with Google for improving Google products and services, enabling technical support, benchmarking, and sharing with Account

---

[270] Hochman Report, ¶ 269.
[271] Declaration of Steve Ganem in Support of Joint Letter Brief Re: Google Preservation, *Rodriguez v. Google*, 3:20-CV-04688, Dkt. 193-1, p. 2-3 (N.D. Cal Dec. 12, 2021).

Specialists."[272] Based on this bare statement and two others of less detail, Mr. Hochman states that he "can infer that Google may have used WAA-off or sWAA-off data to improve particular Google products and services," though he does not name any products or services in particular.[273]

212. There is not sufficient evidence in the record to determine how, if at all, Google uses the specific sWAA-off data at issue to improve any Google product, process, or service in particular, much less to conclude that improving it resulted in monetization of any kind, *e.g.*, advertising profits. Mr. Hochman does not claim otherwise. The two examples he does provide– spam detection and "counterfactuals," are themselves inferences about how these activities at Google *might* use sWAA-off data, but there is no evidence of which I am aware about either subject, and certainly no evidence tying such activity to monetization. Mr. Hochman's opinion as to monetization concerning improvement of products, process, and services is wholly without factual support.

G. Hochman's opinion that Google has collected and saved WAA-off and sWAA-off data in ways that identify class members is inaccurate and unreliable.

213. Mr. Hochman opines that "Google has, throughout the class period, uniformly collected and saved WAA-off and sWAA-off data in ways that identify class members."[274] I disagree. Mr. Hochman lacks factual support for this opinion, and his method of identifying class members is unreliable.

---

[272] Hochman Report, ¶ 297, quoting Google's 4th Supplemental Response to Interrogatory No. 1, Section 7.
[273] Hochman Report, ¶ 298.
[274] Hochman Report, ¶ 343.

214. I understand and agree with Mr. Hochman that "Google maintains a database which reliably shows which Google account holders turned off WAA and sWAA during the class period, and when those users did so."[275] That narrows the potential class to individuals who turned sWAA off. But this is where the line of inquiry ends. Mr. Hochman asserts that "Google can also locate in its records users' devices associated with each Google account, which means that Google knows which of its account holders have used a mobile device during the class period."[276] That is not correct. For this proposition, Mr. Hochman relies on Section VII.B.1 of his report, but that section of his report is merely a description of Google's data infrastructures, and does not discuss whether Google can reliably identify the mobile devices used by every Google account holder with sWAA off at any point during the class period.

215. Mr. Hochman's next paragraph states instead that users can self-identify if they used a mobile device with sWAA off. In this, Mr. Hochman abandons his opinion that Google can identify class members.[277] Mr. Hochman surmises that users can identify a list of apps they've used, and Google can confirm whether the app uses GA4F or AdMob. The problem with this approach is that it does not capture any information about the class member that could be used to determine what conduct, if any, they were exposed to. For example, Mr. Hochman's methodology does not account for:

- app developers who use multiple SDKs;
- users who did not have any private information sent to Google even though they used analytics-enabled apps, within the meaning of Plaintiffs' claims, such that they did not suffer the alleged injury;

[275] Hochman Report, ¶ 344.
[276] Hochman Report, ¶ 345.
[277] Hochman Report, ¶ 349.

- users who never interacted with ads and never triggered a conversion, and therefore could not be said to have generated any revenue for Google under Mr. Hochman's monetization theory;
- users who installed but never used an app;
- how long users used apps, or what types of information they provided the apps;
- what information the users were provided by the apps before they used them, such as privacy policies that discuss Google Analytics;
- users who used apps that never enabled data sharing with Google;
- users who used app that never enabled Google Signals;
- users who reviewed Google's policies and understood Google's anonymization practices.
- Nowhere in his report does Mr. Hochman cite to evidence suggesting that these and other categories of users who are not identical to each other can be identified and their injury quantified using data Google has in its possession. I am aware of no such data.

216. And there is another category of user Mr. Hochman cannot account for – those who had personally identifiable information sent to Google in violation of Google's policies, such as discussed by Mr. Hochman in his report and in my Appendix X2. This type of violation of Google's policies could only have occurred if an app developer programmed the app to send such information to Google and the user interacted with the app in a way that triggered the event to be logged. I am aware of no data or methodology available to determine who would have been affected by this.

217. Mr. Hochman also surmises that, probabilistically, that depending on the number of apps a user has used, a user is almost certain to have used a Firebase-enabled app.[278] But his report does not identify anything further about how those Firebase-enabled apps were configured. It does not account for any of the groups I've identified above, nor for other differences, such as Firebase-enabled apps that do not use analytics, or that do not use conversion measurement, or that do not advertise, or that advertise only with other networks. The list goes on; using a Firebase-enabled app does not, in and of itself, guarantee a user was exposed to the alleged conduct of saving sWAA-off analytics and ads data to a user's Google Account.[279]

218. Mr. Hochman alleges that Google destroyed data that could have been used to identify class members. But he does not identify any destroyed data that would answer the above questions. I render no opinion on whether Google destroyed data that should have been produced, but as to the evidence Mr. Hochman and I both reviewed, there is no indication that Google could have reliably separated class members from non-class-members using data it no longer has; it is my opinion that Google could never have separated class members from non-class members using the class as defined by Plaintiffs and analyzed by Mr. Hochman. Indeed, Mr. Hochman admits that he has "not yet uncovered any information that there is a WAA/sWAA bit for non-GAIA, GA4F logs."[280] I am not aware of any further forthcoming evidence on this subject, so it is unclear why he says he has not yet uncovered any information, but this admission demonstrates at least one fundamental problem with the project of identifying class members as Plaintiffs have defined the class.

---

[278] Hochman Report, ¶ 356, 357.
[279] Mr. Hochman's proposal that users provide their pseudonymous identifiers to Google would solve one problem–that Google cannot link GAIA to IDFA/ADID; but it does not solve the myriad other problems I've identified here.
[280] Hochman Report, ¶ 361.

H. Hochman's opinion that sWAA functioned in ways that were different than Google represented is inaccurate and unreliable.

219. Neither Mr. Hochman nor I are competent to opine on consumer expectations. But as a technical matter, I can and do opine that Google's technology surrounding GA4F and GMA SDK did and does respect the sWAA control as it is written.

220. As Mr. Hochman summarizes, the Google Account Activity Controls page, which is accessible only by entering one's Google Account credentials, offers users to "Choose which settings will save data in your Google Account."[281] The description explains at the top of the page that "The data saved in your account helps give you more personalized experiences across all Google services."[282] Below that, Google reiterates that "You control what data gets saved to your account."[283] One of the controls in question is "Web & App Activity," which offers users the option to "[s]ave[] your activity on Google sites and apps . . . ."[284] The supplemental WAA setting is a checkbox that says "Include Chrome history and activity from sites, apps, and devices that use Google services."[285]

221. Mr. Hochman also details the "Find & Control Your Web & App Activity" help page, which can be reached by clicking "Learn More" on the WAA page. But he leaves out the first paragraph of that help page, which explains:

> If Web & App Activity is turned on, your searches and activity from other Google services are saved in your Google Account, so you may get more personalized

[281] Hochman Report, ¶ 370.
[282] *Id.*
[283] *Id.*
[284] *Id.*
[285] *Id.*

> experiences, like faster searches and more helpful app and content recommendations.[286]

222. Finally, "Google Account" is defined, as I have discussed, as one of fifteen "Key Terms" in Google's Privacy Policy as follows:

> You may access some of our services by signing up for a Google Account and providing us with some personal information (typically your name, email address, and a password). This account information is used to authenticate you when you access Google services and protect your account from unauthorized access by others. You can edit or delete your account at any time through your Google Account settings.[287]

223. And it distinguishes non-PII from personal information as follows:

> **Non-personally identifiable information**
>
> This is information that is recorded about users so that it no longer reflects or references an individually-identifiable user.
>
> **Personal information**
>
> This is information that you provide to us which personally identifies you, such as your name, email address, or billing information, or other data that can be reasonably linked to such information by Google, such as information we associate with your Google Account.

224. Mr. Hochman opines that, as a technical matter, Google does not honor the sWAA promise when the sWAA button is turned to off instead of to on, because, as he argues,

---

[286] "Find & Control your Web & App Activity", Google Account Help, available at https://support.google.com/accounts/answer/54068?hl=en&co=GENIE.Platform%3DAndroid.

[287] "Google Privacy & Terms", Google, available at https://policies.google.com/privacy/key-terms?hl=en-US#toc-terms-account.

the opposite of on would be to save *no* data whatsoever from the user's device when sWAA is off. This is technologically unreasonable because communication between Google, apps, and users are necessary to facilitate the modern operation of mobile devices. It is also not what the descriptions he cites to actually say.

225. Taking his claim literally, as he appears to - that off must be the literal opposite of on – I have considered the question of whether Google does *not* "save to your Google Account," "activity from sites, apps, and devices that use Google services," to provide "more personalized experiences" when sWAA is off. As I have discussed in this report, Google does not do that. Google *will* save to a user's Google Account activity data from apps that use the Google services GA4F and GMA SDK in order to personalize experiences for the user when sWAA is on; when sWAA is off, it does not do that, and it prohibits any Google employee from attempting to do that. And while sWAA off data is still sent to Google by those SDKs, it is pseudonymized and treated as ineligible for personalization or linking to a user's identity, *i.e.*, as non-personally identifiable information, since it "is information that is recorded about users so that it no longer reflects or references an individually-identifiable user."

I. Mr. Hochman mischaracterizes out-of-context Google employee statements.

226. In support of his opinions that sWAA functioned in ways different than Google represented, Mr. Hochman excerpts internal communications between Google employees, which he claims indicates confusion over the settings.[288] Mr. Hochman has taken these statements out of context, or otherwise misrepresented them.

227. Mr. Hochman focused primarily on statements made by Chris Ruemmler, a software engineer working on the "Google Workspace" team responsible for Google first-party

[288] Hochman Report, ¶¶ 380-388.

products like "Calendar," "Gmail," and "Drive." In 2019 and 2020, Mr. Ruemmler sent several emails expressing his opinions on whether Google accurately disclosed to users what happens when WAA is disabled.[289] I disagree with Mr. Hochman's assessment of Mr. Ruemmler's comments and position on the WAA disclosure.

228. First, Mr. Ruemmler admitted during his deposition that he did not work directly on WAA and he has not had any interaction with third-party apps that share data with Google through Google Analytics for Firebase. His sole focus was on first-party apps, "Workspace and Gmail in particular[.]"[290] Therefore, Mr. Ruemmler's emails were not related to the collection of analytics events through third-party apps. Instead, they pertained to Google's direct collection of data through its first-party products like Gmail or Assistant.[291] Additionally, Mr. Ruemmler testified that he mistakenly believed that when WAA was disabled, Google still associated data with a GAIA ID.[292] He was unaware of the extensive anonymization efforts employed by Google to ensure that sWAA-off data is not saved to their GAIA ID.[293] As such, I agree with Mr. Ruemmler's acknowledgment of his "misunderstanding," as he stated, "I didn't know the data was saved anonymously even with WAA off."[294] Because the data is indeed saved anonymously, it is not tied within Google to the user's GAIA identity, or otherwise "saved" to a user's account.

229. The same is true for statements made by J.K. Kearns. Like Mr. Ruemmler, Mr. Kearns only ever worked on first-party products, primarily Google Search, and not on products

---

[289] *See* GOOG-RDGZ-00024709; GOOG-RDGZ-00130381; GOOG-RDGZ-00089546.
[290] Ruemmler Deposition Transcript, at 74:19-24.
[291] *Id*; *see also* 50:15-17.
[292] *Id.* 85:25-86:7.
[293] *Id.* 89:20-90:1
[294] *Id.* 79:18-20.

related to collection from third-party apps. Indeed, Mr. Kearns appears to be so far removed from the practices at issue in this case, that he is only "aware of something called sWAA," which he "think[s] . . . might have something to do with Chrome[.]"[295] His opinions on the functionality of Google Search and WAA cannot be interpreted to say anything as to GA4F and sWAA. But even Mr. Kearns comments themselves cannot be taken as evidence of any internal sentiment. At deposition, he specific that the comments were in the context of "experiments" that Google was running related to the first-party Google Search.[296] Mr. Hochman omitted this necessary context.

230. Mr. Hochman also quotes a comment made by Senior Interaction Designer Elyse Bellamy in a chat exchange, without any context as to the Google Doc that the chat exchange is commenting on.[297] He offers no evidence to conclude this out-of-context quote is relevant to the collection of pseudonymous data through third-party apps.

J. There is no factual basis for Hochman's opinions concerning how Google could change its practices surrounding sWAA-off data.

231. Mr. Hochman opines that Google could change its practices surrounding (s)WAA-off data "so they match their function as described in Google's disclosures" and "do the work that Google says they do."[298] The changes he proposes to achieve this fall into the following three categories: that Google (1) stop "collecting and saving" (s)WAA-off data; (2) purge its systems of (s)WAA-off data already collected, and (3) delete products, services, or

[295] Kearns Deposition Transcript, at 41:19-42:1.
[296] *E.g.*, Kearns Deposition Transcript, at 96:20-22; 86:11-87-16.
[297] Hochman Report, ¶ 388.
[298] Hochman Report, ¶ 409.

algorithms "built in whole or in part" with this data.[299] There is no factual basis for Hochman's opinions concerning how Google could change its practices surrounding (s)WAA-off data. Nor do his proposed changes "ensure" that the WAA and sWAA settings would function as described. As I have discussed throughout this report, Google has the technological infrastructure in place to make sure that they already do; when users turn these personalization settings off, Google does not save any of their activity to their accounts to use it for account personalization. I address each of Mr. Hochman's proposals in more detail below.

232. First, Mr. Hochman opines that Google could change its logging infrastructure "to not save the data" where the Google Analytics for Firebase consent check determines that WAA or sWAA is set to off.[300] And that only then would it "function as advertised." Mr. Hochman takes excerpts from an internal email thread and uses one employee's characterizations of the sWAA control as "a bona fide collection control" as an example of the setting functioning as advertised. The employee does not explain what this means or what the control would entail, and neither does Mr. Hochman. Yet, he uses this stray comment to imply that (s)WAA only works when it stops Google from collecting and saving sWAA-off data, not when it "merely affects how the data is logged."[301] This suggestion demonstrates his misunderstanding of the scope and function of the sWAA setting. As I have discussed throughout this report, the (s)WAA control is a personalization setting. It is not advertised as a data deletion control or as a control that prevents Google from collecting and saving data in "all circumstances." Nor does it function as such. Turning the (s)WAA controls off prevents Google from saving data to a user's account and personalizing their experience accordingly, as advertised.

---

[299] *Id.*
[300] Hochman Report, ¶ 410.
[301] Hochman Report, ¶ 411.

233. Next, Mr. Hochman opines that Google's (s)WAA settings would match their function if Google could simply "not send the data in the first place."[302] To illustrate his point, Mr. Hochman refers to a Firebase product named App Indexing, which is not at issue in this case. A product that the Firebase website describes as "no longer the recommended way of indexing content" and pointing users to "other useful Google developer products."[303] He also references the testimony of Google's product manager for Web &App Activity, to explain how the App Indexing services conducts its consent checks or did at the time of Mr. Monsees's testimony. I am unfamiliar with the product and cannot opine as to the efficacy of the App Indexing product consent checks. But, I will briefly address what Mr. Hochman appears to be proposing—that Google's consent checks should happen on the device instead of Google's servers so that GAIA-tied data is not sent to Google.[304] As I previously stated,, it is my opinion that conducting consent checks at the device level rather than on Google's servers would not result in any change: when sWAA is off, GA4F would still send pseudonymous data to the analytics collection endpoint and it would then be processed for the app developer's analytics uses. Mr. Hochman does not opine that servicing app developer analytics accounts violates privacy, so this use would still need to occur, even if Google made no other use of sWAA-off data.

234. Finally, I address Mr. Hochman's remaining proposals together. Mr. Hochman opines that Google could "change its processes going forward to purge its systems of WAA/sWAA-off data" .[305] Mr. Hochman advances two ways that he thinks Google could do

---

[302] Hochman Report, ¶ 412.
[303] "Firebase App Indexing", Firebase, available at https://firebase.google.com/docs/app-indexing
[304] Hochman Report, ¶ 413.
[305] Hochman Report, ¶ 415.

this. Neither of which would be appropriate under Google's current infrastructure or technologically reasonable.

235. First, Mr. Hochman proposes that Google could populate non-GAIA GA4F logs with a "userControls" field for the purpose of identifying user data/identifiers associated with sWAA-off traffic.[306] He admits that he has not observed a WAA or sWAA bit in non-GAIA, GA4F logs. Yet, he nevertheless makes this proposal based on hypotheticals because he has "observed" this field in a GAIA, GA4F log containing the sWAA bit. To illustrate why he thinks this might work, Mr. Hochman points to field names for 16 AdMob logs that Google produced to Plaintiffs' counsel, which he asserts "reliably track whether the data was generated while WAA or sWAA were off."[307] I am informed by Google counsel that Google described these field names quite differently when it produced them. Plaintiffs' counsel were explicitly told that the fact that a log contains a field that appears to be named in a way that is consistent with being a WAA or sWAA bit does not mean the field is in use, or that it means anything at all. Nevertheless, Mr. Hochman proposes what logs Google could populate for the purpose of identifying user identifiers associated with sWAA-off traffic. He has no factual basis for how Google could identify user data/identifiers associated with sWAA-off traffic. And, without this step, Mr. Hochman has no factual basis for how Google would purge its systems of any particular sWAA-off data using the userControls field or any other field in any logs.

236. Mr. Hochman asserts that "Google could search its systems for all identifiers associated with a user and then delete "traffic" associated with those identifiers for the time when (s)WAA were off."[308] I agree with Mr. Hochman that Google maintains a database that

[306] Hochman Report, ¶ 416.
[307] Hochman Report, ¶ 415.
[308] Hochman Report, ¶ 417.

reliably shows account holders' (s)WAA status. However, as I explained above, his method of identifying sWAA-off data and associating that with specific users is unreliable.

237. Mr. Hochman has no factual basis for his opinion that Google can delete any products, services, or algorithms that it built with (s)WAA-off data. Setting aside his vague and problematic definition of sWAA-off data, and what would be encompassed in Google's "purge," his ideas on how Google can purge its systems of (s)WAA-off data are disconnected from the reality of how Google works and what users expect from these settings. Furthermore, Hochman recommends that Google purge all data without regard to the status of other settings and consents by both end users and Firebase customers, that may affect how this data can be used. His recommendation assumes things about Google's infrastructure that are beyond the scope of this case and what Mr. Hochman and I were asked to opine on.

238. Mr. Hochman is attempting to recreate how the (s)WAA controls function, not match their function to their disclosures. If Google were to accept Hochman's practices, it would no longer do the work Google says they do.

John Black
May 31, 2023